Part III
Computational Number Theory Dr. R.G.E. Pinch
24 lectures Michaelmas Term 1996

The course will cover the mathematics underlying modern computational methods in primality testing and factorisation. The intention is to *prove* results about algorithms as well as describing them.

The prerequisites are elementary number theory (equivalent to the Part IIA course) and some algebraic number theory (at most the Part IIB course). Some knowledge of results from the theory of elliptic curves and of some results from analytic number theory will be useful, but these courses are not prerequisites.

I. *Primality testing*

Fermat, Fermat–Euler and Miller–Rabin ("strong") tests. Conditional polynomial-time methods. Distribution of pseudoprimes and effectiveness of the strong test. P, NP and RP; primes are in NP, composites in RP. Primality proofs. Fermat and Mersenne numbers. The elliptic curve method. Gauss sums and the Cohen–Lenstra method.

II. *Distribution of primes*

Brief sketch of the theory of the Riemann ζ-function and the distribution of primes. Smooth numbers and the Dickman–de Bruijn function.

III. *Factorisation*

Trial division, Fermat's method. Deterministic and random methods. The zero-mod-p and square-root-of-unity classes. Pollard's ρ and $p-1$ methods; Lenstra's elliptic curve method. Dixon's random method; continued fraction and quadratic sieve methods. The multiple polynomial quadratic sieve. The number field sieve. Index calculus and discrete logarithms.

IV. *Cryptography*

Public-key cryptography. Secrecy and authentication. The RSA system. Trap-door functions. Knapsack-based systems. The discrete logarithm problem and el Gamal (DSA) signatures.

Reading

The computational aspects are covered by the following, of which [1] has copious references.

1 H. Riesel *Prime numbers and computer methods for factorisation*, 2nd ed, Birkhauser 1994.

2 N. Koblitz *A course in number theory and cryptography* Springer 1987.

3 H. Cohen *Computational number theory* Springer 1993.

RGEP 24 May 1996.

Computational Number Theory.

1. Primality Testing.

Recall: A prime number p has the property $a|p \Rightarrow a = \pm 1, \pm p$ (irreducible).
Euclidean algorithm shows that this implies $p|ab \Rightarrow p|a$ or $p|b$ (prime).

Euclid's Algorithm: $\text{hcf}(a,b) = \text{hcf}(a-b, b) = \cdots = \text{hcf}(a - qb, b) = \text{hcf}(r, b)$, where $a = qb + r$, $0 \le r < b$. So write:

$$\begin{aligned} a &= q_1 b + r_1, & 0 \le r_1 < b \\ b &= q_2 r_1 + r_2, & 0 \le r_2 < r_1 \\ &\vdots & \vdots \\ r_{n-1} &= q_{n+1} r_n + r_{n+1}, & \text{and } r_{n+1} = 0. \end{aligned}$$

Then, $\text{hcf}(a,b) = \cdots = \text{hcf}(r_n, 0) = r_n$.

Easy to see that $r_{i+2} \le \frac{1}{2} r_i$, all i. Hence $n = \#\text{steps} \le 1 + 2\log_2 b$.

Proof: $\left.\begin{aligned} r_{i-1} &= q_{i+1} r_i + r_{i+1} \\ r_i &= q_{i+2} r_{i+1} + r_{i+2} \end{aligned}\right\}$ Now, $\left.\begin{aligned} r_{i+1} &\ge r_{i+2} \\ q_{i+2} &\ge 1 \end{aligned}\right\} \Rightarrow r_i \ge r_{i+1} + r_{i+2} > 2 r_{i+2}$.

Exercise: Show that # steps can be at least $\log_\varphi b$, where $\varphi = \frac{1+\sqrt{5}}{2}$ (Hint: Fibonacci numbers).
So, the algorithm runs in time polynomial in # bits in input - a "polynomial-time" algorithm.

Theorem (Euclid): There are infinitely many primes.
Proof: Multiply together and add 1.

Quantitative version, due to Euler:
Theorem: $\sum_p \frac{1}{p}$ diverges. Indeed, $\sum_{p \le x} \frac{1}{p}$ is approximately $\log\log x$. (cf: $\sum_{n \le x} \frac{1}{n} \sim \log x$).

Legendre, Gauss, Chebyshev, etc, conjectured that $\pi(x) = \#\{p \le x\}$ is about $x/\log x$.
Riemann's memoir introduced the zeta-function, $\zeta(s) = \sum_n \frac{1}{n^s}$ ($s \in \mathbb{C}$), and gave an 'explicit' formula: $\pi(x) = \text{Li}(x) - \text{Li}(x^{1/2}) + \cdots + \sum_\rho \frac{x^\rho}{\rho} +$ remainder, where $\text{Li}(x) = \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}$, and ρ runs over non-trivial zeroes of $\zeta(s)$. Riemann Hypothesis: $\text{Re}(\rho) = 1/2$.

Hadamard and de la Vallée Poussin proved the Prime Number Theorem: $\pi(x) \sim \text{Li}(x) \sim x/\log x$.
Riemann Hypothesis (if true) $\Rightarrow \pi(x) = \text{Li}(x) + O(x^{\frac{1}{2}+\varepsilon})$.

Recall: $g = O(f)$ means $\exists K$ such that $|g(x)| \le K|f(x)|$, and $O(f)$ denotes any such g.

Probabilistic Primality Tests.

Let $L(N) = \#$ bits in N. An algorithm is polynomial time if the number of elementary operations is $\le L(N)^k$ (some k), and exponential time if $\le N^k$.
An algorithm is randomised if there is some random choice in the working, and we talk about expected time. Otherwise, it is deterministic - ie, the calculation is always identical for identical N.

An algorithm is probabilistic if the output could be one of prime, composite, probably prime, probably composite.

First algorithm: trial division.
Test every factor t from 2 to $N-1$. If $t|N$, then N is composite. If not, N is prime.
Of course, we need only test t up to $\sqrt{N}$.
This is clearly an exponential-time algorithm, full deterministic and not probabilistic.
The algorithm furnishes a certificate of compositeness, which can be checked in polynomial time.

Fermat Criterion.
This uses Fermat's Little Theorem: if p is prime and $(b,p)=1$ then $b^{p-1} \equiv 1 \pmod p$
The test: take $1<b<N$. If $(b,N) \neq 1$, N is composite. If $b^{N-1} \not\equiv 1 \pmod N$, N is composite.
Otherwise, N is "probably" prime.

steps in Euclid for (b,N) is polynomial. In $b^{N-1} \pmod N$? Firstly, work mod N all the time. We can find $(b \bmod N)^{N-1}$ in time $L(N)$ by squaring: take $b, b^2, b^{2^2}, b^{2^3}, \ldots$ and combine powers corresponding to bits in $N-1$ ("Peasant method")
Hence, the test is polynomial-time.

Variations: choose b at random mod N, or fix a specific b, say 2. How good is the test? Ie, how often will composite N have the property $b^{N-1} \equiv 1 \pmod N$, some b's?
Dickson claimed that the Chinese thought $2^{N-1} \equiv 1 \bmod N \Rightarrow N$ prime, but there is no evidence for this. Since the first pseudoprime to base 2, ie composite N such that $2^{N-1} \equiv 1 \pmod N$, is 341, it is unlikely anyone would have seriously proposed this.
So, $N<341$ and $2^{N-1} \equiv 1 \bmod N \Rightarrow N$ is prime.
Up to 10^{13}, there are 264,239 pseudoprimes (psps) to base 2, and 346,065,536,839 primes.

$N = 341 = 31 \times 11$ is a Fermat psp base 2, but $3^{340} \bmod 341 = 56$, so 341 is composite.
Unfortunately, consider $N = 561 = 3 \times 11 \times 17$. We find that $b^{N-1} \equiv 1 \bmod N$ whenever $(b,N)=1$. So the only way the Fermat criterion fails is when b has a factor in common, so here the criterion is as hard to use as trial division.

Given N, let $W(N) = \{b \bmod N : b^{N-1} \equiv 1\}$. Clearly, $W(N)$ is a subgroup of $(\mathbb{Z}/N)^*$.
So either $W(N) = (\mathbb{Z}/N)^*$, or $|W(N)| \leq \frac{1}{2}|(\mathbb{Z}/N)^*| = \frac{1}{2}\varphi(N)$.
So either $W(N) = (\mathbb{Z}/N)^*$, or $\frac{|W(N)|}{N} \leq 1/2$.

We call N for which $W(N)$ is $(\mathbb{Z}/N)^*$ a Carmichael number.
So if N is not a Carmichael number then choosing b uniformly at random gives the right answer with probability $> 1/2$.

The exponent of a group is the maximum order of any element = least m such that $g^m = 1$ for all $g \in$ group. So exponent | order.

Lemma: Let $(\mathbb{Z}/n)^*$ be the multiplicative group. The order is $\varphi(n)$, where φ is Euler's totient function, and the exponent is $\lambda(n)$, where $\lambda(p_1^{e_1}\cdots p_r^{e_r}) = \operatorname{lcm}\{\lambda(p_i^{e_i})\}$, and $\lambda(p^e) = \varphi(p^e)$ for p odd, and $\lambda(2)=1$, $\lambda(4)=2$, $\lambda(2^e) = 2^{e-2}$, $e\geq 3$.

Proof: $(\mathbb{Z}/p_1^{e_1}\cdots p_r^{e_r})^* \cong (\mathbb{Z}/p_1^{e_1})^* \times \cdots \times (\mathbb{Z}/p_r^{e_r})^*$. If p is odd, $(\mathbb{Z}/p^e)^*$ is cyclic, so $\lambda(p^e) = \text{order} = \varphi(p^e)$. If $p=2$, for $e\geq 3$, $(\mathbb{Z}/2^e)^*$ satisfies $(\mathbb{Z}/2^e)^* \cong \langle 5\rangle \times \langle -1\rangle$.

Sublemma: $(\mathbb{Z}/2^e)^* \cong \langle 5\rangle \times \langle -1\rangle$

Proof: (i) $(\mathbb{Z}/2^e)^*$ is not cyclic
(ii) 5 has order exactly 2^{e-2}
} Prove by induction on $e\geq 3$.

Suppose true for e. $\exists$ map $(\mathbb{Z}/2^{e+1})^* \to (\mathbb{Z}/2^e)^*$ which is surjective, namely reduction mod 2^e. And, $(\mathbb{Z}/2^e)^*$ not cyclic $\Rightarrow$ $(\mathbb{Z}/2^{e+1})^*$ not cyclic, so (i) is true for $e+1$.
We have $5^{2^{e-3}} \neq 1 \bmod 2^e$, but $5^{2^{e-2}} \equiv 1 \bmod 2^e$. By induction again, $5^{2^{e-3}} \equiv 1 \bmod 2^{e-1}$
So $5^{2^{e-3}} = 1 + \varepsilon.2^{e-1}$, ε odd. So, $5^{2^{e-2}} = 1 + 2\varepsilon.2^{e-1} + \varepsilon^2.2^{2(e-1)} = 1 + \varepsilon.2^e + \varepsilon^2.2^{2e-2}$.
Now, $e\geq 3$, so $2e-2 > e$. So $5^{2^{e-2}} \equiv 1 + \varepsilon.2^e \bmod 2^{e+1}$, and $5^{2^{e-1}} \equiv 1 + 2\varepsilon.2^e \equiv 1 \bmod 2^{e+1}$.
So 5 mod 2^{e+1} has order exactly 2^{e-1}.

A number is Carmichael if $\lambda(n) \mid n-1$.

Proposition (Korsfeld): Odd n is Carmichael iff n is squarefree, composite and $p\mid n \Rightarrow p-1 \mid n-1$.

Proof: n is odd. $p^2 \mid n \Rightarrow p \mid \lambda(p^2) \mid \lambda(n)$ and so $p^2 \mid n \Rightarrow \lambda(n) \nmid n-1$. So for squarefree n, $\lambda(n) = \operatorname{lcm}_{p\mid n}\{p-1\} \mid n-1 \iff p-1 \mid n-1$ for all $p\mid n$.

Let $n = 561 = 3\times 11\times 17$. So, $3-1\mid 560$, $11-1\mid 560$, $17-1\mid 560$, so n is Carmichael.

* **Theorem:** There are infinitely many Carmichael numbers. Indeed, if $C(x) :=$ number of them $\leq x$, then $x^{2/7} < C(x) < x\exp\left(-(1-\varepsilon)\log x \log\log\log x / \log\log x\right)$, for large x. *

Compare: $\pi(x) \sim x\exp(-\log\log x)$, so Carmichael numbers are 'rare' compared to primes.
Chernik forms: First example. $(6k+1)(12k+1)(18k+1) = n$ is Carmichael if each factor is prime.
Easy to check $n = 1 + 36k(\cdots)$, so if $p = 6k+1$, $q = 12k+1$, $r = 18k+1$, all prime, then $p-1$, $q-1$, $r-1$ all divide $n-1$. Eg, $k=1$, $n = 7.13.19 = 1729$. A very difficult conjecture, Schinzel's Hypothesis, implies (as trivial corollary) that there are infinitely many Carmichael numbers.

From now on, consider n odd only.

Proposition: Probability of the Fermat test incorrectly returning prime (for random b mod n) is $w(n) = \frac{1}{\varphi(n)} \cdot \prod_{p\mid n} \operatorname{hcf}(p-1, n-1)$.

Proof: Ring $\mathbb{Z}/n \cong \oplus(\mathbb{Z}/p_i^{e_i})$, where $n = \prod p_i^{e_i}$ (Chinese Remainder Theorem).
In particular, $(\mathbb{Z}/n)^* \cong \oplus(\mathbb{Z}/p_i^{e_i})^*$, and n odd $\Rightarrow$ each factor $(\mathbb{Z}/p^e)^*$ is cyclic.
solutions to $b^{n-1} \equiv 1 \bmod n$ is the product of the # solutions of $b^{n-1} \equiv 1 \bmod p^e$, ie. in cyclic group of order $p^{e-1}(p-1)$. But $\operatorname{hcf}(p^{e-1}, n-1) = 1$, so # solutions to $b^{n-1} \equiv 1$ in each factor is $\operatorname{hcf}(p-1, n-1)$. So overall # solutions is $\prod \operatorname{hcf}(n-1, p-1)$, and $w = \frac{1}{\varphi(n)} \cdot$ this number.

Euler Criterion.

First improvement: observe $n-1$ is even, so $b^{n-1} = (b^{\frac{n-1}{2}})^2 \bmod n$.

Lemma: Equation $x^2 \equiv 1 \bmod n$ has 2^r solutions, where r = # distinct prime factors of n.

Proof: $(\mathbb{Z}/n)^* = \bigoplus_{i=1}^{r} (\mathbb{Z}/p_i^{e_i})^*$, and # solutions to $x^2 \equiv 1$ is product of # solutions for each factor, ie 2^r.

So, **Euler criterion** is: $b^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$.

Example: $2^{644} \equiv 1 \bmod 645$, so 645 is a psp base 2 for Fermat, but $2^{322} \equiv 259 \bmod 645$. So the Euler test strictly includes the Fermat test. Note incidentally that $2^{322} \equiv 1 \bmod 129$, and $\equiv -1 \bmod 5$. So in this case, obtain a factor of n for free.

Remark: if $x^2 \equiv 1 \bmod n$ but $x \not\equiv \pm 1$, then $x+1$, $x-1$ have factors in common with n, so apply Euclid to form $\text{hcf}(n, x \pm 1)$ - finds factors in polynomial time.
The converse is true - ie, given factors of n, one can find $x \not\equiv \pm 1$ with $x^2 \equiv 1$.

What about Carmichael numbers? Unfortunately, $n = 1729 = 7.13.19$ satisfies $b^{864} \equiv 1 \bmod 1729$ for all $(b, 1729) = 1$
Lehman and Leech / Jaeschke / Davenport Jr. observed that repeated application of Euler's criterion can reveal compositeness, since they proved that if a Carmichael number always passes the Euler test, it must do so with $b^{\frac{n-1}{2}} \equiv +1$. So if this happens say 20 times, see event of very low probability for n prime, so better to answer composite. We shall see later that this is a bad idea.

Euler-Jacobi Criterion.

Next improvement: identify ± 1 in Euler test. If n is prime, then $b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \bmod n$, where $\left(\frac{b}{n}\right)$ is the Legendre symbol, defined as: $\left(\frac{b}{n}\right) = \begin{cases} 0 & \text{if } n \mid b \\ +1 & \text{if } b \equiv x^2 \bmod n, \text{ some } x \\ -1 & \text{if } b \not\equiv x^2 \bmod n, \text{ any } x. \end{cases}$

Define the **Jacobi symbol** for odd positive $n = \prod p_i^{e_i}$ to be $\left(\frac{b}{n}\right) = \prod \left(\frac{b}{p_i}\right)^{e_i}$.
Clearly, $\left(\frac{b \bmod n}{n}\right) = \left(\frac{b}{n}\right)$ and $\left(\frac{b}{n_1 n_2}\right) = \left(\frac{b}{n_1}\right)\left(\frac{b}{n_2}\right)$. From properties of the Legendre symbol, $\left(\frac{b_1 b_2}{n}\right) = \left(\frac{b_1}{n}\right)\left(\frac{b_2}{n}\right)$, $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$, $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.
To prove these two results, we need to check that maps $\varphi(n) = (-1)^{\frac{n-1}{2}}$, $w(n) = (-1)^{\frac{n^2-1}{8}}$ are (totally) multiplicative, on odd n, ie $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$, $w(n_1 n_2) = w(n_1) w(n_2)$
Finally, we have the **Law of quadratic reprocity**: if m, n both odd and positive, then $\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2} \cdot \frac{m-1}{2}} \cdot \left(\frac{n}{m}\right)$

Claim that $\left(\frac{b}{n}\right)$ can be computed in polynomial time (in $\log b$, $\log n$), indeed, by a slight extension of Euclid's algorithm.

Warning: $\left(\frac{x^2}{n}\right) = +1$, but $\left(\frac{b}{n}\right) = +1 \not\Rightarrow b \equiv$ square $\bmod n$.

So, Euler-Jacobi criterion is: $b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \bmod n$, where $\left(\frac{b}{n}\right)$ is the Jacobi symbol, and both sides of the test are computable in polynomial time.
Again, there are psps, eg $2^{170} \equiv +1 \bmod 341$, but $\left(\frac{2}{341}\right) = -1$, so fails the EJ test.
Finally, we have a criterion with no analogue of Carmichael numbers.

Proposition: Let $w_{EJ}(n)$ = proportion of bases b such that n passes the EJ test base b.
Then $w_{EJ}(n) \leq 1/2$ if n composite.

Proof: Observe that the sets of b which pass the Fermat, Euler, EJ tests are subgroups of $(\mathbb{Z}/n)^*$ in each case, and so $w_{EJ}(n) \leq w_E(n) \leq w_F(n)$.
If n is not a Carmichael number, then $w_F \leq \frac{1}{2}$ already. So it is sufficient to show result for n Carmichael. Further, it suffices to find just one base b such that $(b,n)=1$ and b fails the EJ test. So take n Carmichael, ie $n = p_1 p_2 \cdots$, with $p_i - 1 \mid n-1$, each i.
Case (i): $\frac{n-1}{p-1}$ is even for all $p \mid n$, ie $p-1 \mid \frac{n-1}{2}$ for all $p \mid n$.
Then $b^{\frac{n-1}{2}} \equiv 1 \bmod p_i$, all p_i, so $b^{\frac{n-1}{2}} \equiv 1 \bmod n$. But there exists b such that $\left(\frac{b}{n}\right) = -1$, say $\left(\frac{b}{p_1}\right) = -1$ and $b \equiv 1 \bmod p_2 p_3 \cdots$. Then $\left(\frac{b}{n}\right) = \prod \left(\frac{b}{p_i}\right) = -1$, so $b^{\frac{n-1}{2}} \not\equiv \left(\frac{b}{n}\right) \bmod n$.
Case (ii): $\frac{n-1}{p_1 - 1}$ is odd, say. Then choose b such that $\left(\frac{b}{p_1}\right) = -1$ and $b \equiv 1 \bmod p_2 p_3 \cdots$
Then $b^{\frac{n-1}{2}} = b^{\frac{p_1-1}{2} \cdot \frac{n-1}{p_1-1}} \equiv (-1)^{\text{odd}} \bmod p_1$. But $b^{\frac{n-1}{2}} \equiv 1^{(\cdots)} \bmod p_2 p_3 \cdots$,
so $b^{\frac{n-1}{2}} \not\equiv \pm 1 \bmod n$. So b fails the Euler test.
So in each case, we find $b \bmod n$ which fails EJ or E part of test.

Classification of algorithms: Consider problems with yes/no answers in properties of input numbers n. The instance of problem is n expressed in binary. Property is in class P (polynomial) if there is an algorithm which returns answer 'Yes' (if that is the answer) in time $< L^K$, where L = # bits in n and K is a constant. A problem is in class NP (non-deterministic polynomial) if there is an algorithm, given n and a suitable auxiliary number g, gives the answer 'Yes' (if that is the answer) in time $< L^K$, where L is the length of n + length of g in bits. Finally, a property is in class RP (random polynomial) if in class NP, and a fixed proportion α of all guesses will give answer.

For example, compositeness is NP, with g a factor of n.
Another interpretation of g is that it is a certificate or proof of answer.

Corollary of proposition: Compositeness is in class RP, with guess or certificate for composite n a base b such that n fails EJ test. ($\alpha = 1/2$).

Clearly, $P \subseteq RP \subseteq NP$. The classes co-P, co-RP, co-NP are defined as above with 'Yes' replaced by 'no'. Easy to see that $P = \text{co-}P$. For, if n does not have the property, wait time $L^K + 1 < L^{K+1}$. If answer 'yes' has not emerged, we know answer must be 'no'.

* Theorem: $NP \neq \text{co-}NP$ and $RP \neq \text{co-}RP$, unless $P = NP$, when all classes are equal. *.

We shall later show that primeness is in NP, ie prime & composite $\in$ NP $\cap$ co-NP.
Indeed, primeness $\in$ RP.

Miller-Rabin Test

We can do better by returning to the idea that $\sqrt{1} = \pm 1$ when n is prime. For odd n, $n-1$ is even, and so consider $b^{\frac{n-1}{2}}$. If $n \equiv 1 \bmod 4$ and $b^{\frac{n-1}{2}} \equiv 1$, then $b^{\frac{n-1}{4}}$ ought to be ± 1
So, let $n = 1 + 2^r \cdot s$, with s odd, and form the Miller-Rabin sequence (mod n):
$b^s, b^{2s}, \ldots, b^{2^{r-1}\cdot s} \left(= b^{\frac{n-1}{2}}\right), b^{2^r \cdot s} \left(= b^{n-1}\right)$. The MR test, or "strong test" for n is that the sequence either begins with 1, or the first occurrence of 1 is preceded by -1.
If not, n is composite.
However, there are still pseudoprimes. Eg, $N = 4033 = 37 \cdot 109$, but $N-1 = 2^6 \cdot 63$, and
$2^{63} = 3521$, $2^{2\cdot 63} = -1$, $2^{4\cdot 64} = +1, \ldots$

Obviously, the MR test includes the Fermat and Euler criteria. We shall prove that it includes the EJ criterion, and that $w_{MR}(n) \leq 1/4$ if n is composite.
So, MR test is strictly stronger than the EJ test. (Eg, $n = 1105$)

Let $n = \prod p_i^{a_i}$, $p_i - 1 = 2^{r_i} s_i$, $n-1 = 2^r s$. Define $O_2(b \bmod m)$ = power of 2 dividing the order of b in multiplicative group $(\mathbb{Z}/m)^*$. b satisfies MR criterion if: (i) order of $(b \bmod p_i^{a_i})$ divides $n-1$,
(ii) $O_2(b \bmod p_i^{a_i})$ is the same $\forall i$.

If so, call this the Level of b. So, level $0 \Rightarrow b^s = +1$,
level $1 \Rightarrow b^s = -1$, $b^{2s} = +1$.

Finally, note that $(\mathbb{Z}/p^a)^* \to (\mathbb{Z}/p)^*$, reduction mod p, gives that for p odd, $O_2(b \bmod p^a) = O_2(b \bmod p)$. So (ii)' reads: $O_2(b \bmod p_i)$ same $\forall p_i | n$.

Proposition: If b satisfies MR criterion mod n, then b also satisfies EJ criterion.

Proof: Assume b satisfies MR and hence Euler criterion. Need to prove $\left(\frac{b}{n}\right) \equiv b^{\frac{n-1}{2}} \bmod n$.
Let l = level of b, ie $b^{2^l \cdot s} \equiv 1$, $b^{2^{l-1}\cdot s} \equiv -1$ if $l > 0$. (Assume this)
Certainly, $2^l | p_i - 1$, so put $p_i = 1 + 2^l t_i \bmod 2^{l+1}$, with $t_i = 0$ or 1.
$\left(\frac{b}{p_i}\right) = 1 \iff O_2(b \bmod p_i) <$ power of 2 in $p_i - 1 \iff t_i = 0$.
Now, $n = \prod p_i^{a_i} \equiv \prod (1 + 2^l t_i)^{a_i} \bmod 2^{l+1} \equiv 1 + (\sum t_i a_i) 2^l \bmod 2^{l+1} = 1 + T \cdot 2^l \bmod 2^{l+1}$, say.
And, $\left(\frac{b}{n}\right) = \prod \left(\frac{b}{p_i}\right)^{a_i} = \prod (-1)^{t_i a_i} = (-1)^T$. We have $n - 1 \equiv T \cdot 2^l \bmod 2^{l+1}$, so
$T = 0$ if $2^{l+1} | n-1$, and $= 1$ if $2^l \| n-1$.
Now, -1 appears in $(l-1)^{th}$ place in the MR sequence, ie at $b^{\frac{n-1}{2}}$ if $2^l \| n-1$, and otherwise before $b^{\frac{n-1}{2}}$ in sequence.
So $b^{\frac{n-1}{2}} = -1 \iff 2^l \| n-1 \iff T = 1 \bmod 2 \iff \left(\frac{b}{n}\right) = -1$, so EJ criterion holds.
If $l > 0$: Then, $O_2(b \bmod p_i)$ is odd, ie $\left(\frac{b}{p_i}\right) = +1$, all p_i. So $\left(\frac{b}{n}\right) = \prod \left(\frac{b}{p_i}\right)^{a_i} = 1 = b^{\frac{n-1}{2}}$.

So MR test includes EJ test and is stronger.
Eg: $n = 6601 = 7 \cdot 23 \cdot 41$, and $2^{1650} \equiv 4509$, $2^{3300} \equiv 1$, $2^{6600} \equiv 1$, and $\left(\frac{2}{n}\right) = +1$.

Corollary: When $n \equiv 3 \bmod 4$, MR criterion = E criterion = EJ criterion.

Proposition: There are infinitely many MR-pseudoprimes base 2.

Proof: If n is a Fermat psp base 2, then $N = 2^n - 1$ is a MR-psp base 2. For:
If n is a Fermat psp, then in particular it is composite, say $n = ab$. Then $2^a - 1$ is a non-trivial factor of $2^n - 1 = N$, so N is composite.
$N - 1 = 2^n - 2 = 2(2^{n-1} - 1) = 2s$, say, s odd. Now, $2^{n-1} \equiv 1 \bmod n$ as it is a Fermat psp, so $n \mid s$, hence $2^s \bmod N$ is a power of $2^n \bmod N$, ie of $1 \bmod N$. So $2^s \equiv 1 \bmod N$.

Proposition: Let n have d distinct prime factors. The proportion of bases which pass the MR test is at most 2^{1-d} times the proportion which pass the Fermat test.
ie: $w_{MR}(n) \leq w_F(n) \cdot 2^{1-d}$.

Proof: Write $n = \prod p_i^{a_i}$, $n - 1 = 2^r \cdot s$, $p_i - 1 = 2^{r_i} s_i$, with s, s_i odd. Let $c_i(l)$ = proportion of $b \bmod p_i^{a_i}$ for which $o_2(b \bmod p_i) = l$. So $c_i(0) = 2^{-r_i}$, $c_i(l) = 2^{l-1-r_i}$, $1 \leq l \leq r_i$, $c_i(l) = 0$ for $l > r_i$.
Proportion of bases passing test at level l is $w_F(n) \cdot \prod_{i=1}^{d} c_i(l)$.
So $w_{MR}(n) = w_F(n) \cdot \sum_{l=0}^{r} \prod_{i=1}^{d} c_i(l) = w_F(n) \cdot S$, say. Put $R = \Sigma r_i$ and $\rho = \min\{r, r_i\}$.
Now, $\prod_{i=1}^{d} c_i(l) = 2^{-R}$ for $l = 0$ (and $l = 1$)
$= 2^{dl - R - d}$ for $l \geq 1$, $l \leq \rho$.
$= 0$ for $l > \rho$.
So $S = 2^{-R}\left(1 + \sum_{l=1}^{\rho} 2^{d(l-1)}\right) = 2^{-R}\left(1 + \frac{2^{d\rho} - 1}{2^d - 1}\right)$. Note $R \geq \rho d \geq d \geq 1$.
Now, $2^R + 2^1 \geq 2^{R-a} + 2^{1+a}$ for $0 \leq a \leq R - 1$. So $2^R + 2 \geq 2^{R+1-d} + 2^d$.
So $2^{R+1} + 2 \geq 2^R + 2^{R+1-d} + 2^d$. Now, $2^{\rho d} - 1 \leq 2^R - 1 \leq 2^{R+1} - 2^d - 2^{R+1-d} + 1 = (2^d - 1)(2^{R+1-d} - 1)$,
hence $\frac{2^{\rho d} - 1}{2^d - 1} \leq 2^{R+1-d} - 1$. So $S \leq 2^{-R}(1 + 2^{R+1-d} - 1) = 2^{1-d}$.

Corollary: For $n > 9$, composite, $w_{MR}(n) \leq \frac{1}{4}$.

Proof: If $d = 1$, then $n = p^a$, some $a \geq 2$. $w_F(n) = \frac{\text{hcf}(n-1, \varphi(n))}{\varphi(n)} = \frac{p-1}{n-1} = \frac{1}{1 + p + \cdots + p^{a-1}} \leq \frac{1}{p + a - 1} < 1/4$.
If $d = 2$, then n cannot be Carmichael, so $w_F(n) \leq \frac{1}{2}$ and $w_{MR}(n) \leq \frac{1}{2} w_F \leq 1/4$.
If $d \geq 3$, then $w_{MR}(n) \leq \frac{1}{4} w_F \leq 1/4$.

Remark: The case n = prime power is easy to detect. If $n = p^a$, then $a < \log n$, so there are at most $\log n$ possible a, and each could be checked in polynomial time.

Randomised algorithm: choose $b \bmod n$ uniformly at random and check MR criterion base b. This has probability $< 1/4$ of giving wrong answer if n composite.
Deterministic algorithm: might choose $b = 2, 3, 5$.

Theorem: If the Extended Riemann Hypothesis (ERH) holds, then any proper subgroup of $(\mathbb{Z}/n)^*$ must omit at least one number of any consecutive list of $2(\log n)^2$ numbers.

Theorem: If ERH holds, then n is prime if it satisfies MR test for $b = 2, \ldots, \lceil 2(\log n)^2 \rceil$.

Corollary: If ERH holds, then "primeness" $\in P$.

2. Primality Tests On Ranges Of Numbers

Let $\mathcal{M}_k$ = sample space of all odd k-bit numbers with uniform probability.

$\mathcal{A}(n)$ = event "n is input to algorithm"

Y_t = event "n passes t rounds of MR test"

$\mathcal{C}$ = event "n is composite"

$\mathcal{P}$ = event "n is prime."

We want $w(t,k) := \mathbb{P}(\mathcal{C} \mid Y_t)$. We know $\mathbb{P}(Y_1 \mid \mathcal{C}) \le 1/4$, so $\mathbb{P}(Y_t \mid \mathcal{C}) \le 4^{-t}$. (Assume bases chosen randomly mod n). Need to apply Bayes' Theorem: $\mathbb{P}(\mathcal{C} \mid Y_t) = \frac{\mathbb{P}(\mathcal{C} \cap Y_t)}{\mathbb{P}(Y_t)}$, given $\frac{\mathbb{P}(\mathcal{C} \cap Y_t)}{\mathbb{P}(\mathcal{C})} \le \frac{1}{4^t}$. So need $\mathbb{P}(\mathcal{C})$ and $\mathbb{P}(Y_t)$.

Theorem: (i) $p(n) \gg n \log n$, $p(n)$ the nth prime.

(ii) $1.105\, x/\log x \gg \pi(x) \gg x/\log x$ for $x > 10^6$.

(iii) $\mathbb{P}(\mathcal{P}) \gg \frac{2.5}{k}$ for $k \gg 50$.

Find subset $\mathcal{E}_m$ of $\mathcal{C}$ such that if n is composite, not in $\mathcal{E}_m$, then $\mathbb{P}(Y_1 \mid \mathcal{A}(n)) \le 2^{-m}$, and show $\mathcal{E}_m$ is small.

Proposition: For $k \gg 50$ and $2 \le m \le \sqrt{k/2}$, there are subsets $\mathcal{E}_m$ of $\mathcal{C}$ such that

(i) for $n \in \mathcal{C} \setminus \mathcal{E}_m$, $\mathbb{P}(Y_1 \mid \mathcal{A}(n)) \le 2^{-m}$

(iii) $\mathbb{P}[\mathcal{E}_m] \le (1.02)\cdot 2^{2m - k/m}$ [(ii) is in printed notes].

Proof: Let $X = 2^k$, so $|\mathcal{M}_k| = \frac{1}{4}X$. Let $A = 2^{m-1}$, $\delta = 1/m$, $Y = \frac{1}{2}X^{\delta}$. Since $k \gg 50$, $\delta k \gg \sqrt{2k} \gg 10$, and so $Y \gg \frac{1}{2}\cdot 2^{10} = 512$. Let $n \in \mathcal{C}$, $n = \prod_{i=1}^{d} p_i^{q_i}$. Let $c_i = \text{hcf}(p_i - 1, n-1)$, $b_i = \frac{p_i - 1}{c_i}$.

So, $w_F(n) = \frac{1}{\varphi(n)} \cdot \prod c_i = \frac{1}{n} \cdot \prod \frac{p_i}{b_i}$. Define $\mathcal{E}_m = \{ n \in \mathcal{C} : b_i < A$, some $p_i \mid n$ with $p_i > Y \}$.

(i) Want to show: if $n \in \mathcal{C} \setminus \mathcal{E}_m$ then $w_{MR}(n) \le 2^{-m}$.

If $d > m$ then $w_{MR}(n) \le 2^{1-d} w_F(n) \le 2^{-m}$. So suppose $d \le m$ and $n \notin \mathcal{E}_m$.

(a) Suppose all $p_i < Y$. Let $D = \prod p_i$. So $\frac{n}{D}$ is coprime to $n-1$ (as n is).

But $\frac{n}{D}$ divides $\varphi(n) = \frac{n}{D} \cdot \prod (p_i - 1)$.

Now, $D \le Y^d \le Y^m$ and $n > \frac{1}{2}X$, so $\frac{n}{D} \gg \frac{n}{Y^m} = n/(\frac{1}{2}X^{\delta})^m \gg \frac{\frac{1}{2}X}{2^{-m}X} = 2^{m-1}$.

Now, $w_F(n) \le \frac{D}{n} \le 2^{1-m}$, and $w_{MR}(n) \le \frac{1}{2} \cdot w_F = 2^{-m}$.

(b) $\exists\, p_i \mid n$ with $p_i > Y$, but $b_i \gg A$. Then $w_F(n) \le \frac{p_i}{n} \cdot \frac{1}{b_i} \le \frac{1}{A} = 2^{1-m}$, and $w_{MR}(n) \le 2^{-m}$, as in (a).

(iii) Fix $p > Y$, and suppose $n \in \mathcal{E}_m$ because $p \mid n$ and $b = \frac{p-1}{\text{hcf}(p-1, n-1)} < A$. Then $n \equiv 0 \bmod p$, and $n \equiv 1 \bmod c = \text{hcf}(p-1, n-1)$. So $n \equiv p \bmod pc$. The number of such n in $\mathcal{M}_k$ is at most $\frac{\frac{1}{2}X}{pc} + 1 - 1 = \frac{1}{2}X \cdot \frac{b}{p(p-1)}$.

Sum over $p > Y$ and $b < A$: $|\mathcal{E}_m| \le \sum_{p>Y} \sum_{b<A} \frac{\frac{1}{2}Xb}{p(p-1)} = \frac{1}{2}X \sum_{p>Y} \frac{1}{p(p-1)} \sum_{b<A} b < \frac{1}{2}X \sum_{p>Y} \frac{1}{p(p-1)} \cdot \frac{1}{2}A^2$.

Estimate $\sum_{p>Y} \frac{1}{p(p-1)} < \sum_{\text{odd } n > Y} \frac{1}{n(n-1)} = \sum_{\text{odd } n > Y} \frac{1}{n-1} - \frac{1}{n} < \left(\frac{Y+1}{Y-1}\right)^2 \cdot \frac{1}{2} \cdot \frac{1}{Y-1} < \frac{0.505}{Y}$

So, $\frac{|\mathcal{E}_m|}{|\mathcal{M}_k|} \le \frac{1}{4}A^2 X \cdot \frac{0.505}{Y} \cdot \frac{1}{\frac{1}{4}X} < (1.02)\cdot 2^{2m - k/m}$.

Compare with some data: for $k = 51$ and $m = 3$, we have $|\mathcal{E}_3| \le 2^{34.84}$.

Direct computation: there are $32055 < 2^{15}$ numbers in $\mathcal{M}_{51}$ with $w_{MR} \gg 1/8$.

Proposition: For $3 \le v \le \sqrt{k/2}$, $w(t,k) = \mathbb{P}(\mathcal{C} \mid Y_t) \le \frac{1}{\mathbb{P}(P)} \cdot \left(\sum_{m=3}^{v} \mathbb{P}(\mathcal{E}_m) \cdot 2^{-t(m-1)} + 2^{-tv} \right)$.

Proof: We have $\mathcal{E}_{m-1} \subseteq \mathcal{E}_m \subseteq \cdots$, so $\mathbb{P}(\mathcal{C} \mid Y_t) = \mathbb{P}(\mathcal{E}_3 \mid Y_t) + \sum_{m=4}^{v} \mathbb{P}(\mathcal{E}_m \setminus \mathcal{E}_{m-1} \mid Y_t) + \mathbb{P}(\mathcal{C} \setminus \mathcal{E}_v \mid Y_t)$.

$= \left[\mathbb{P}(\mathcal{E}_3 \cap Y_t) + \sum \mathbb{P}((\mathcal{E}_m \setminus \mathcal{E}_{m-1}) \cap Y_t) + \mathbb{P}((\mathcal{C} \setminus \mathcal{E}_v) \cap Y_t) \right] / \mathbb{P}(Y_t)$.

Now, $\mathbb{P}(\mathcal{E}_3 \cap Y_t) = \mathbb{P}(Y_t \mid \mathcal{E}_3) \cdot \mathbb{P}(\mathcal{E}_3) \le 2^{-2t} \cdot \mathbb{P}(\mathcal{E}_3)$

$\mathbb{P}((\mathcal{E}_m \setminus \mathcal{E}_{m-1}) \cap Y_t) = \mathbb{P}(Y_t \mid \mathcal{E}_m \setminus \mathcal{E}_{m-1}) \cdot \mathbb{P}(\mathcal{E}_m \setminus \mathcal{E}_{m-1}) \le 2^{-t(m-1)} \cdot \mathbb{P}(\mathcal{E}_m)$

$\mathbb{P}((\mathcal{C} \setminus \mathcal{E}_v) \cap Y_t) = \mathbb{P}(Y_t \mid \mathcal{C} \setminus \mathcal{E}_v) \le 2^{-vt}$.

And, $P \subseteq Y_t$, so $\frac{1}{\mathbb{P}(P)} \ge \frac{1}{\mathbb{P}(Y_t)}$. Substituting $\Rightarrow$ result.

Theorem: For $k \ge 50$, if $1 \le t \le 4$: $w(t,k) \le 0.4k \cdot (1+2^t) \cdot 2^t \cdot 2^{-t\sqrt{k/2}}$

$5 \le t \le \frac{k}{9} + 2$: $w(t,k) \le 0.4k \cdot 2^t \left(2^{-2\sqrt{k(t-2)}} + 2^{-t\sqrt{k/2}} \right)$

$t > \frac{k}{9} + 2$: $w(t,k) \le 0.4k \cdot 2^t \left(2^{6-3t-k/3} + 2^{-t\sqrt{k/2}} \right)$.

Proof: Let $M = \lfloor k/2 \rfloor$. Put $v = M$ in previous proposition and get:

$\mathbb{P}(\mathcal{C} \mid Y_t) \le \frac{1}{\mathbb{P}(P)} \left(\sum_{m=3}^{M} \mathbb{P}(\mathcal{E}_m) \cdot 2^{-t(m-1)} + 2^{-tM} \right)$.

Now, $2^{-tm} \le 2^{-t(\sqrt{k/2}-1)}$. By lemma, $\frac{1}{\mathbb{P}(P)} \le 0.4k$. And, $\sum_{m=3}^{M} \mathbb{P}(\mathcal{E}_m) \cdot 2^{-t(m-1)} \le \frac{(1.2)2^t}{\sqrt{2k}} \cdot \sum_{m=3}^{M} 2^{(2-t)m - k/m}$.

So let $S = \sum_{m=3}^{M} g(m)$, where $g(m) = 2^{(2-t)m - k/m}$.

If $1 \le t \le 4$: $g(m)$ increases for $3 \le m \le M$. So $S \le M g(M) \le \sqrt{k/2} \cdot 2^{-t\sqrt{k/2}}$.

$5 \le t \le \frac{k}{9} + 2$: $g(m)$ attains maximum at $m_0 = \sqrt{k/(t-2)}$ and $3 \le m_0 \le M$.

So $S \le M g(m_0) \le \sqrt{k/2} \cdot 2^{-2\sqrt{k(t-2)}}$.

$t > \frac{k}{9} + 2$: $g(m)$ decreases for $m \ge 3$. So $S \le M g(3) \le \sqrt{k/2} \cdot 2^{6-3t-k/3}$.

Example: $k = 250$ (about 75 decimal digits), $t = 6$. $w(6, 250) \le 2^{-56}$.

The improved theorem with $k = 1000$, $t = 10$ gives $w(10, 1000) \le 2^{-165}$.

3. Primality Proofs.

Basic idea: n is prime if it has a primitive root, ie an element of order exactly $n-1$ in the multiplicative group.

Proposition: Suppose $n-1 = \prod_{i=1}^{d} q_i^{e_i}$ and there exist a_i, $i = 1, \ldots, d$ such that $a_i^{n-1} \equiv 1 \bmod n$ and $\mathrm{hcf}\{n, a_i^{\frac{n-1}{q_i}} - 1\} = 1$, then n is prime.

Proof: Conditions imply that $a_i^{n-1} \equiv 1 \bmod p$ and $a_i^{\frac{n-1}{q_i}} \not\equiv 1 \bmod p$ for any $p \mid n$, so the exponent of the multiplicative group mod p is at least $n-1$, ie $n-1$ is the order of some subgroup of $(\mathbb{Z}/p)^\times$. So $n-1 \mid p-1$; in particular $n \le p$, so n is prime.

Theorem: The property "n is prime" is in NP.

Proof: Let $l = \log_2 n$. Claim there is a certificate of primeness of n of length $\le 2l^3$ bits, which can be checked in polynomial time. Assume $l \ge 4$. Our certificate consists of a list (a_i, q_i, C_i), where C_i is a certificate of primality of q_i. Proceed by induction. Let $d = \#$ distinct prime factors of $n-1$, $d < l$. Let $l_i = \log_2 q_i$, so length of $C_i \le 2l_i^3$. Assume n odd, so $n-1$ even, $\sum_{i>1} l_i < l-1$, and omit C_1 from list.

So, $\sum_{i=2}^{d} 2l_i^3 \le 2(\sum l_i)^3 \le 2(l-1)^3 = 2(l^3 - 3l^2 + 3l - 1) \le 2(l^3 - 2l^2 - l)$. So total length of certificate $\le 2(l^3 - 2l^2 - l) + 2l(l+1) = 2l^3$. Check that each line is checkable in polynomial time. Hence "n is prime" is in NP.

Consider $P = 2.10^{63} + 2.10^{36} + 2.10^{12} + 2293$.

$P-1 = 2^2 . 3 . 83 . 293 . 4759 . P_{13} . Q$, where Q is probably prime.

See printed notes for the process.

Fermat Numbers.

Define $F_n = 2^{2^n} + 1$. So $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$. But $F_5 = 641 \times 6700417$.

$F_n - 1 = 2^{2^n}$, so we can prove F_n prime (if it is) by finding a such that $(a^{\frac{F_n-1}{2}} - 1, F_n) = 1$ and $a^{F_n - 1} \equiv 1 \mod F_n$.

So we have F_n is prime $\Leftrightarrow$ passes Euler criterion with $a^{\frac{F_n-1}{2}} \equiv -1 \mod F_n$.

Expect $(\frac{a}{F_n}) = -1$, so we look for such a: since $F_n \equiv 1 \mod 4$ $(n \geq 1)$, $\equiv 2 \mod 3$ $(n \geq 1)$, we have $(\frac{F_n}{3}) = -1$, so $(\frac{3}{F_n}) = -1$. Hence F_n is prime $\Leftrightarrow 3^{2^{n-1}} \equiv -1 \mod F_n$.

Theorem: Suppose $n-1 = FC$, where $(F, C) = 1$ and $F = \prod_{i=1}^{d} q_i^{e_i}$ and there exist a_i such that $a_i^{n-1} \equiv 1 \mod n$ and $\text{hcf}\{a_i^{\frac{n-1}{q_i}} - 1, n\} = 1$.

Then every $p \mid n$ satisfies $p \equiv 1 \mod F$.

Proof: As before, there is a subgroup of $(\mathbb{Z}/p)^*$ of order F.

Corollary: If $F > C$ then n is prime.

Proposition: Let $n-1 = 2^r s$, with $2^r > s$. If n passes the MR test base b with $b^{\frac{n-1}{2}} \equiv -1 \mod n$ then n is prime.

"Uprun": If $\mathcal{L}$ is a list of proved primes, write F = product of elements of $\mathcal{L}$, and set $n = FC + 1$ $(C < F)$. If n passes MR test, worth trying to prove n is prime.

Heuristic: such numbers have frequency $x/(\log x)^2$ near x.

Primality proofs showed 'primeness' is in NP.

Theorem (Adleman, Huang): 'Primeness' is in RP.

The quadratic ring $(\mathbb{Z}/n)[\sqrt{d}]$ is $\mathbb{Z}[x]/\langle n, x^2 - d\rangle$, ie $\{x + y\sqrt{d} : x, y \in \mathbb{Z}/n\}$.

Clearly this is a ring. It is a field iff (i) n is prime, (ii) d is not a square in $\mathbb{Z}/n$, ie $(\frac{d}{n}) = -1$.

Invertible elements: Define the norm $N(x+y\sqrt{d}) = (x+y\sqrt{d})(x-y\sqrt{d}) = x^2 - dy^2$.

Then $(x+y\sqrt{d})^{-1} = \frac{x-y\sqrt{d}}{x^2-dy^2}$ if norm is invertible mod n. The map $x+y\sqrt{d} \mapsto x-y\sqrt{d}$ is an automorphism of the ring.

In the case $n = p$, prime, $(\mathbb{Z}/p)[\sqrt{d}]$ is either:

$\cong \mathbb{Z}/p \oplus \mathbb{Z}/p$, if $d = e^2 \mod p$, with $(x+y\sqrt{d}) \mapsto (x+ye, x-ye)$, or

$\cong GF(p^2)$, the field of p^2 elements, if $(\frac{d}{p}) = -1$

The multiplicative group of $\mathbb{Z}/p \oplus \mathbb{Z}/p$ is $C_{p-1} \oplus C_{p-1}$ of exponent $p-1$ and order $(p-1)^2$.

That of $GF(p^2)$ is cyclic, of order $p^2 - 1$.

Map $\alpha \mapsto \alpha^p$ is an automorphism of the field, called Frobenius, and so must be $\sqrt{d} \mapsto -\sqrt{d}$. So norm $(x+y\sqrt{d})(x-y\sqrt{d})$ is just $\alpha \mapsto \alpha^{p+1}$.

So $N : GF(p^2)^* \to GF(p)^*$ is $(p+1):1$, so is surjective.

$\alpha \longmapsto \alpha^{p+1}$

We call $GF(p)^*$ the rational part of $GF(p^2)^*$, and the quotient group $GF(p^2)^*/GF(p)^*$ of order $p+1$ is the corational group. Kernel of norm map is nearly the same.
Map: $\ker N \hookrightarrow GF(p^2)^* \to$ corational has kernel order 2.

The Fermat criterion translates into an assertion about the corational group.
Given n, pick $d \bmod n$. If $\text{hcf}(d,n)>1$, n is factored. Pick $\beta = x+y\sqrt{d}$.
If $\text{hcf}(N(\beta), n)>1$, n is factored. Otherwise consider β^n.
If n is prime and $\left(\frac{d}{n}\right) = -1$ then $\beta^n = x - y\sqrt{d}$. If $\left(\frac{d}{n}\right) = +1$ then $\beta^n = \beta$.

Lucas Criterion
This is: $(x+y\sqrt{d})^n \equiv x + \left(\frac{d}{n}\right) y\sqrt{d}$. If n is prime, Lucas criterion holds.
When $\left(\frac{d}{n}\right) = +1$, this is just the Fermat test done twice, ie Fermat criterion for bases $x \pm ye$ $(e^2 \equiv d \bmod n)$ simultaneously. If $\left(\frac{d}{n}\right) = -1$, then Lucas test is Fermat condition for rational and corational groups simultaneously.

Suppose β passes test and $b = \beta\bar{\beta} = N(\beta)$. Lucas $\Rightarrow \beta^N = \bar{\beta}$, so $\bar{\beta}^N = \bar{\bar{\beta}} = \beta$, so $b^n = (\beta\bar{\beta})^n = \bar{\beta}\beta = b$, so $b^{n-1} \equiv 1 \bmod n$. And $(\beta/\bar{\beta})^{n+1} = \beta\bar{\beta}/\bar{\beta}\beta = 1$, so $(\beta/\bar{\beta})^{n+1}$ has norm 1, hence $=1$ in the corational group.
Lucas test is often expressed in terms of $\beta = x+y\sqrt{d}$, with $N(\beta)=1$, since there is a faster method for squaring norm 1 elements: $(x+y\sqrt{d})^2 = x^2 + y^2 d + 2xy\sqrt{d} = 2x^2 - (x^2 - y^2 d) + 2xy\sqrt{d} = (2x^2 - 1) + 2xy\sqrt{d}$.

Lucas psps can be constructed from Fermat psps. Set $n = 341 = 31 \times 11$, $d = 5$, $\beta = 3 + 212\sqrt{5} \bmod 341$.
Then, $\left(\frac{5}{341}\right) = +1$ and $\beta^{341} = \beta$. Since $5 \equiv 37^2 \bmod 341$, $3 + 212\sqrt{5} \mapsto (3 + 212.37, 3 - 212.37) \equiv (4, 2) \bmod 341$.
There are also absolute pseudoprimes, analogous to Carmichael numbers.
Let $n = 17.31.41.43.89.97.167.331$. This has the property that $p \mid n \Rightarrow p^2 - 1 \mid n-1$.
So for any $\left(\frac{d}{n}\right) = +1$, we have $\beta^n = \beta.\beta^{n-1} \equiv \beta(\beta^{p^2-1}) \equiv \beta \bmod p$, and fails for any $\left(\frac{d}{n}\right) = -1$.

We can see that if n has more than one prime factor there will always be values of d for which the Lucas criterion fails. Consider $n = 2465 = 5.17.29$, and put $d = 3$.
$\left(\frac{3}{2465}\right) = -1$. $\beta = -73 + 226\sqrt{3}$ satisfies $\beta^n \equiv \bar{\beta} \bmod n$.
Consider n with property $p \mid n \Rightarrow p+1 \mid n+1$, eg $(6k-1)(12k-1)(18k-1)$, say $5.11.17$ for more examples.

We can now proceed to proofs analogous to the previous ones, based on the corational group, and factorising $n+1$ rather than $n-1$.

Proposition: Let $n+1 = FC$ with $F = \prod_{i=1}^{d} q_i^{e_i}$ and $(F,C) = 1$. If there exists d, with $\left(\frac{d}{n}\right) = -1$ and $\beta_1, \ldots, \beta_d \in (\mathbb{Z}/n)[\sqrt{d}]$ of norm 1 with the property $\beta_i^{n+1} \equiv 1 \bmod n$ and $\text{hcf}\{\beta_i^{(n+1)/q_i} - 1, n\} = 1$, then every prime factor $p \mid n$ satisfies $p \equiv \left(\frac{d}{p}\right) \bmod F$.
In particular, if $F > C$ then n is prime.
(Here, $\text{hcf}(\alpha - 1, n) = 1$ means $\text{hcf}(N(\alpha - 1), n) = 1$).

Proof: Let p divide n. The conditions on β_i imply there is a subgroup of order F in $(\mathbb{Z}/p)[\sqrt{d}]^*$, which is of exponent $p - \left(\frac{d}{p}\right)$, ie $p \equiv \left(\frac{d}{p}\right) \bmod F$.

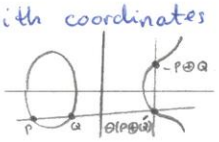
Mersenne Numbers.

$M_p = 2^p - 1$. If p is composite, M_p is too, hence we may assume p is prime.
Need to find d such that $\left(\frac{d}{M_p}\right) = -1$, and β not a square in the corational group.
$M_p \equiv 1 \bmod 3$, $\equiv -1 \bmod 4$, so $\left(\frac{3}{M_p}\right) = -1$, so take $d = 3$. Can see $\beta = 2+\sqrt{3}$ is of norm 1.
Since $M_p \equiv -1 \bmod 8$, 2 is a square $\overset{\text{mod } M_p}{\lambda}$, and find $\beta = \gamma^2$, where $\gamma = \frac{1+\sqrt{3}}{\sqrt{2}}$ has norm -1.
If M_p is prime, then $\beta^{\frac{M+1}{2}} = \gamma^{M+1} = \gamma\bar{\gamma} = -1$. Hence $\beta = 2+\sqrt{3}$ will be the desired element if M_p is prime. So M_p is prime iff $\beta^{\frac{M+1}{2}} \equiv -1 \bmod M_p$, ie, iff $\beta^{2^{p-1}} \equiv -1 \bmod M_p$.

Interlude:- Elliptic Curves.

An elliptic curve over a field F is a (non-singular) plane cubic
$E: Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$.
If $\mathrm{char}\, F \neq 2$, can take $a_1 = a_3 = 0$; in $\mathrm{char}\, F \neq 3$, can take $a_2 = 0$.
In characteristic 0, often take $Y^2 = 4X^3 - g_2X - g_3$.
As well as affine points, there is one point $\mathcal{O}$ "at infinity", ie $(0:1:0)$ in projective coordinates.

If K is a field containing F, let $E(K)$ be the set of points on E (including $\mathcal{O}$) with coordinates in K. Define a relation on $E(K)$ by: $P \oplus Q \oplus R = 0 \iff P, Q, R$ collinear.



Two points with the same x-coordinate are collinear with $\mathcal{O}$, so call them $P, \ominus P$. If we define $P \oplus Q$ as $\ominus R$, where R is the unique point such that P, Q, R are collinear. (Note, R is in $E(K)$).

Theorem: $E(K)$ is an abelian group with identity $\mathcal{O}$. (Associativity follows as the sum of two points is defined by rational functions of the coordinates of P, Q).

Let $F = GF(q)$ be a finite field. There are at most q^2+q+1 points in $\mathbb{P}^2(F)$, so $E(F)$ is finite. $\#E(F) = \underset{\text{point at } \infty}{1} + \sum_{x \in F} \underset{\text{\# roots of } y^2 = x^3+ax+b}{(0,1,2)} \sim 1+q$ (heuristic). Define $t = 1+q - \#E(F)$.

Theorem: $|t| \leq 2\sqrt{q}$.

Theorem: Every value of t permitted by this inequality occurs. Indeed, the number of curves corresponding to t is $H(t^2-4q)$, where $H(d) = \#$ primitive binary quadratic forms of discriminant d.

If $t = 0$ (more generally, if $p \mid t$ where $p = \mathrm{char}\, F$), the curve is called supersingular.
When $t = 0$, the group $E(F)$ of order $p+1$ is either the corational group, or is (norm 1 group)$/(\pm) \oplus C_2$. So we concentrate on the non-supersingular case.
Such curves are always complex multiplication curves, ie $\mathrm{End}_{\bar{F}}(E) \cong$ a subring of $\mathbb{Z}[\sqrt{d}]$, where in fact $d = t^2 - 4q$. We can construct such curves for small d ("Atkin curves"), by considering $E_d = \mathbb{C}/\Lambda$, where Λ is a lattice in $\mathbb{Z}[\sqrt{d}]$, which is

an elliptic curve over $\mathbb{C}$, which is defined over an algebraic number field containing $\mathbb{Q}(\sqrt{d})$. "Hilbert class field."

So if $\mathfrak{q}$ is a prime ideal $|q$, then $E \bmod \mathfrak{q}$ is an elliptic curve over F with $q+1-t$ points, where $d = t^2 - 4q$.
In the other direction, given E and F, we need to compute the order of $E(F)$.
We defined an Atkin curve as a complex multiplication curve with 'small' d.

Example: $E: Y^2 = X^3 + X$. Map $\tau: (x,y) \mapsto (-x, iy)$, $i^2 = -1$, is an automorphism of order 4.
$\tau^2: P \mapsto \ominus P$. Endomorphism ring of E contains (indeed is) $\mathbb{Z}[\tau] \cong \mathbb{Z}[i]$.
Over $F = GF(p)$, E again has $\mathbb{Z}[i]$ in endomorphism ring (over separable closure).
- If $p \equiv 3 \bmod 4$, E is supersingular. $\#E(F) = p+1$. (endomorphism ring is quaternion algebra).
- If $p \equiv 1 \bmod 4$, can write $p = a^2 + 4b^2$. $\#E(F) = p+1-a$.
  $E^{(-1)}: Y^2 = X^3 - X$ ("twisted") has $p+1+a$ points.

Let n be any number $\equiv 1 \bmod 4$. First step is to solve $n = a^2 + 4b^2$. Find d such that $\left(\frac{d}{n}\right) = -1$. Then $d^{\frac{n-1}{2}}$ should be -1 (EJ test for n). Put $c = d^{\frac{n-1}{4}}$. $c^2 \equiv -1 \bmod n$.
Now, $n \mid (c+i)(c-i)$ in $\mathbb{Z}[i]$, which is a Euclidean Domain, so we find $\text{hcf}(n, c+i) = a+ib$ in $\mathbb{Z}[i]$, by Euclid's Algorithm. So $a \pm ib \mid n$, so $a^2+b^2 = n$ (or (a,b) is a non-trivial factor of n). Choose a odd, b even.

Remark: Selection of d is equivalent to the corresponding choice in MR method, ie, expected time is 2, on ERH $2(\log n)^2$, otherwise power of n.

Second step: consider elliptic curves $E^{\pm}: Y^2 = X^3 \pm X$, with orders $n+1 \pm a$. Select points at random on $E^{\pm}$. If $[n+1 \pm a]P \neq \mathcal{O}$, (ie, $[n+1]P \neq [\pm a]P$), then n is composite, else probably prime.

This is (a form of) Elliptic Fermat's Criterion.

We can extend this method to a proof of primality. Idea is to prove that a point on E mod n has the required order. The group structure of E over a finite field is of the form $C_a \oplus C_b$ where $a \mid b$ and $ab = \#E$, and a is a factor of $|F^*|$ ("Weil pairing").
Suppose E is an elliptic curve whose order mod n is $n+1-t$ if n is prime, that $n+1-t = FC$, where $F = \prod_{i=1}^{d} q_i^{e_i}$, $(F, C) = 1$ and $F > C$. Suppose further that for each $q_i \mid F$, there are points P_i, Q_i and integers a_i, b_i such that $a_i + b_i = e_i$, $[q_i^{a_i}]P_i = [q_i^{b_i}]Q_i = \mathcal{O}$, and $[q_i^{a_i-1}]P \neq \mathcal{O}$, $[q_i^{b_i-1}]Q \neq \mathcal{O}$, (in the sense that the denominators of coefficients are coprime to n).
Then n is prime.
Proof: Conditions imply that if $p \mid n$, $E(GF(p))$ has subgroups of order $q_i^{a_i+b_i} = q_i^{e_i}$, so $F \mid \#E(GF(p))$. Now, $\sqrt{n} < F < \#E \bmod p < (\sqrt{p}+1)^2$. So $\sqrt{p}+1 > \sqrt[4]{n}$, hence $p > n$.

This is the basis of Morain's ECPP program. (and Provable Prime Q function in Mathematica). ECPP can routinely prove primality of numbers of ~3000 digits.

Sketch Proof that 'primeness' is in RP.

Idea is that 'many' curves have 'smooth' order. A number is smooth if all its prime factors are small. If we could prove that there were many smooth numbers in the range $p \pm \sqrt{p}$, say, then EC method would have a 'high' chance of succeeding.
Adleman/Huang replaced 'EC' by 'Abelian Surface', where crucial range is $p^2 \pm p^{3/2}$

Distribution of Pseudoprimes.

Let $P(x)$ = # base 2 psps $\le x$, ie, # $\{ n$ composite : $2^{n-1} \equiv 1 \bmod n \}$.
Define $L(x) = \exp(\log x \log\log\log x / \log\log x)$. We stated that $\frac{P(x)}{x} \le L(x)^{-\frac{1}{2}+\varepsilon}$, and $\frac{C(x)}{x} \le L(x)^{-1+\varepsilon}$, where $C(x)$ = # Carmichael numbers $\le x$.
Define $\ell_2(n)$ = order of 2 in the multiplicative group of n. So n is a Fermat psp iff $\ell_2(n) \mid n-1$. Aim to show that $\frac{P(x)}{x} \le L(x)^{-1/2}$ for $x \ge x_0$.

Proposition: For $x \ge x_0$, $\#\{ m \le x : \ell_2(m) = n \} \le x \cdot \exp\left[-\log x \cdot \frac{3 + \log\log\log x}{2 \log\log x} \right]$

Proof: Assume $x \ge n$. For $c > 0$, we are estimating:

$$\sum_{\substack{m \le x \\ \ell_2(m)=n}} 1 \le \sum_{\ell_2(m)=n} (x/m)^c = x^c \sum_{\ell_2(m)=n} m^{-c} \le x^c \sum_{p|m \Rightarrow \ell_2(p) | n} m^{-c} = x^c \sum_{p_1,\dots,p_t} (p_1^{e_1} \cdots p_t^{e_t})^{-c} = x^c (1 + p_1^{-c} + p_1^{-2c} + \dots)(1 + p_2^{-c} + p_2^{-2c} + \dots) \cdots$$
$$= x^c \prod_{p : \ell_2(p) | n} (1 - p^{-c})^{-1}$$

Choose $c = 1 - \frac{4 + \log\log\log x}{2 \log\log x}$, and x_0 such that $c \ge 7/8$.
Write $A = \prod_{\ell_2(p) | n} (1 - p^{-c})^{-1}$ for given c. Result will follow if we can show that $\log A = o(\log x / \log\log x)$, since $\# \le x^c A = \exp(c \log x + \log A) = \exp\left(\log x \left(1 - \frac{4 + \log\log\log x}{2 \log\log x} \right) + \log A \right)$
Estimate $\log A$: $\log(1+t) = t + O(t^2)$ for $t < 1$
So that $\log \prod_p (1 - p^{-c})^{-1} = -1 \cdot \sum_p \log(1 - p^{-c}) = \sum_p (p^{-c} + O(p^{-2c})) = \left(\sum_p p^{-c} \right) + O\left(\sum_p p^{-2c} \right)$
But $\sum_p p^{-2c}$ is a subseries of $\sum_n n^{-2c}$, and $2c \ge 7/4$, so $\sum_n n^{-2c} \le \zeta(7/4)$, so $O(\cdots)$ is just $O(1)$.
So $\log A = \sum_{\ell_2(p) | n} p^{-c} + O(1) = \sum_{d | n} \sum_{\ell_2(p) | d} p^{-c} + O(1)$
We want to examine $\{ p : \ell_2(p) = d \}$. Such p must divide $2^d - 1$, hence there are $< d$ of them. Say they are $q_1, \dots, q_t$, $t < d$.
Now, $q_i \equiv 1 \bmod d$ (as $d \mid q_i - 1$), so $q_i \ge 1 + d_i$. So, $\sum_{\ell_2(p) = d} p^{-c} \le \sum_{i=1}^{d-1} (1+id)^{-c} < d^{-c} \sum_{i=1}^{d-1} i^{-c}$.
Compare $\sum_{i=1}^{d-1} i^{-c}$ with $\int_1^d t^{-c}\,dt$: $\sum_{i=1}^{d-1} i^{-c} < \int_1^d t^{-c}\,dt = \left[\frac{t^{1-c}}{1-c} \right]_1^d < \frac{d^{1-c}}{1-c}$.
So, $\sum_{\ell_2(p)=d} p^{-c} < \frac{d^{1-2c}}{1-c}$.
So $\log A < \sum_{d | n} \frac{d^{1-2c}}{1-c} + O(1) < \frac{1}{1-c} \sum_{m = \prod p\text{'s with } p | n} m^{1-2c} + O(1) = \frac{1}{1-c} \prod_{p | n} (1 - p^{1-2c})^{-1} + O(1)$

Now, we need to estimate $B = \prod_{p | n} (1 - p^{1-2c})^{-1}$. Note $1 - 2c < -3/4$.
$\log B = -\sum_{p | n} \log(1 - p^{1-2c}) = \sum_{p | n} p^{1-2c} + O(1) \le \sum_{p \le y} p^{1-2c} + O(1)$, where y will be specified.
Method for estimating $\sum_{p \le x} f(p) = \sum_{m \le x} f(m) \cdot [1 \text{ if } m \text{ is prime}] = \int_1^x f(t)\,d\pi(t)$, as a Riemann-Stieltje integral.
Integrate by parts: $\sum_{p \le x} f(p) = [f(t)\pi(t)]_1^x - \int_1^x f'(t)\pi(t)\,dt$, and approximate by PNT: $\pi(x) \sim \frac{x}{\log x}$.
Here, $\sum_{p \le y} p^{1-2c} = [t^{1-2c} \cdot \pi(t)]_1^y - (1-2c) \int_1^y t^{-2c} \cdot \pi(t)\,dt < 1.105 \cdot \frac{y^{1-2c} \cdot y}{\log y} \cdot \frac{1}{4}$.

Now, y is chosen so that $p \mid n \Rightarrow p \le y$. Choose y so that $\prod_{p \le y} p > x$, then this suffices to replace $\sum_{p \mid n}$ by $\sum_{p \le y}$. We can take $y = 2\log x$ for this.
So, $\log \prod_{p \mid n} (1-p^{1-2c})^{-1} \ll (\log x)^{2-2c}/2(1-2c)\log\log x$, where $\ll$ means "$<$ a multiple of".
$\log A \le \frac{1}{1-c} \cdot \prod_{p \mid n} (1-p^{1-2c})^{-1} + O(1)$. So $\log\log A \ll (\log x)^{2-2c}/(2-2c)\log\log x$.
Finally, substitute $c = 1 - \frac{4+\log\log\log x}{2\log\log x}$, and get $\log A < \frac{2\log\log x}{4+\log\log\log x} + O(1)$
$= o(\log x / \log\log x)$

We used steps: • $\sum_{m \text{ composed of } p_1, \dots, p_t} m^{-s} = \prod_{i=1}^{t} (1-p_i^{-s})^{-1}$
• $\sum_{p \le x} f(p) = [f(t).\pi(t)]_1^x - \int_1^x f'(t).\pi(t)\,dt$.
• correct choice of c at the end.

Theorem: $\frac{P(x)}{x} \le L(x)^{-1/2}$

Plan: Split up psps into classes: $(n \le x)$
(i) $n \le x/L(x)$
(ii) $\exists\, p \mid n$ with $b_2(p) \le L(x)$ and $p > L(x)^3$
(iii) $\exists\, p \mid n$ with $b_2(p) > L(x)$
(iv) the rest.

Proof: (i) # psps n in case (i) is clearly $\le x/L(x)$.
(ii) # p with $b_2(p) \le L(x)$ is: $\sum_{m \le L(x)} \sum_{b_2(p)=m} 1 \le \sum_{m \le L(x)} \sum_{p \mid 2^m - 1} 1 \le \sum_{m \le L(x)} m \le L(x)^2$
So # psps in class (ii) is:
$\le \sum_{\substack{p > L(x)^3 \\ b_2(p) \le L(x)}} x/p \le \frac{x}{L(x)^3} \cdot \sum_{p : b_2(p) \le L(x)} 1 \le \frac{x}{L(x)^3} \cdot L(x)^2 = x/L(x)$.

(iii) If n is a psp and $d \mid n$ then $n \equiv 0 \bmod d$, $n \equiv 1 \bmod b_2(d)$, as $b_2(d) \mid b_2(n) \mid n-1$, and so $(d, b_2(d)) = 1$. So, # psps n with $n \le x$ and $d \mid n$ is $\le 1 + \frac{x}{d.b_2(d)}$.
But if d is a prime $p \mid n$, then $n \equiv 0 \bmod p$, $n \equiv 1 \bmod b_2(p)$, and $b_2(p)$ is a factor of $n-1$. So $n \equiv p \bmod p(p-1)$, so $n \equiv p \bmod p b_2(p)$.
So # psps with $p \mid n$ and $n \le x$ is $\le 1 + \frac{x}{p.b_2(p)} - 1$ (as $n = p$ is not a psp), ie, $\le \frac{x}{p.b_2(p)}$.
So # psps $n \le x$ with $p \mid n$ and $b_2(p) > L(x)$ is $\le \sum_{\substack{2 \le p \le x \\ b_2(p) > L(x)}} \frac{x}{p.b_2(p)} < \frac{x}{L(x)} \cdot \sum_{p \le x} \frac{1}{p}$.
We need to calculate: $\sum_{p \le x} 1/p$
$= \int^x \frac{1}{t}\,d\pi(t) = \left[\frac{1}{t}\pi(t)\right]^x + \int^x \frac{1}{t^2}\pi(t)\,dt < 1.2\left(\frac{1}{x} \cdot \frac{x}{\log x} + \int^x \frac{1}{t^2} \cdot \frac{t}{\log t}\,dt\right) = 1.2\left(\frac{1}{\log t} + \int^x \frac{1}{\log t}\,d\log t\right)$
$= 1.2\left(\frac{1}{\log x} + \log\log x\right)$
So # psps in class (iii) is $< 2\frac{x}{L(x)}\log\log x$.

(iv) If n is a psp in class (iv) then n has a divisor d with $\frac{x}{L(x)^4} < d \le \frac{x}{L(x)}$ $-(*)$, since each prime factor $p < L(x)^3$. Let d run over odd numbers in this range.
So, # psps $\le \sum_d^* \left(1 + \frac{x}{d.b_2(d)}\right) \le \frac{x}{L(x)} + x \sum_d^* \frac{1}{d.b_2(d)} \le \frac{x}{L(x)} + x \sum_{m \le x} \sum_{d : b_2(d) = m}^* \frac{1}{dm}$.
Now, $\sum_{b_2(d)=m}^* \frac{1}{d} \le \frac{L(x)^4}{x} \cdot \#\{d\text{'s in range}\} \le \frac{L(x)^4}{x} \cdot x \exp\left(-\log x \cdot \frac{3+\log\log\log x}{2\log\log x}\right) =: F(x)$
So, # psps in (iv) $\le x \cdot \sum_{m \le x} \frac{1}{m} \cdot F(x) \le x(\log F(x)) = x.L(x)^4.\log x.\exp\left(-\log x \cdot \frac{3+\log\log\log x}{2\log\log x}\right)$
$= x.\exp\left(\log\log x + \frac{4\log x \log\log\log x}{\log\log x} - \frac{3\log x}{2\log\log x} - \frac{\log x \log\log\log x}{2\log\log x}\right)$ — should be $-\frac{1}{2}$ (see handout)
$= x.\exp\left(\frac{\frac{1}{2}(\log\log x)^2 + 7\log x \log\log\log x - 3\log x}{2\log\log x}\right) < x.\exp\left(\frac{\frac{7}{2}(1+\varepsilon)\log x \log\log\log x}{\log\log x}\right) < x/L(x)^{1/2}$
So (assume correct result), # in each class $< \frac{x}{L(x)}, \frac{x}{L(x)}, \frac{x}{L(x)}, \frac{x}{L(x)^{1/2}}$, so $P(x) < \frac{x}{L(x)^{1/2}}$

2. Factorisation

We can divide methods into three classes:
(i) Trial division : Fermat's method (difference of squares), Lehman's method.
(ii) Zero-mod-p methods: Pollard's ρ, $p\pm1$ methods, Lombard's elliptic curve method.
(iii) Square-root-of-1 methods: (Fermat's method), Dixon's factor base method, quadratic sieve, multiple polynomial QS, number field sieve, (special and general)

We consider algorithms both deterministic and randomised. Analysis of running time falls into three types: Heuristic (relies on the special function being "like random")
Expected.
Deterministic.

Trial division based methods

If n is the number to be factored, factors could be as large as $\sqrt{n}$, so trial division could take time $O(\sqrt{n})$. The worst case for TD is the class of RSA numbers $n=pq$, $p\simeq q$.
Fermat's method: write $n=a^2-b^2$. We may assume n is odd. If $n=a^2-b^2=(a+b)(a-b)$, done.
The method is to systematically test $n+b^2$ for being square. When $n+b^2=a^2$, done.
Computation can be speeded up by congruence considerations.
This works well when TD works badly, ie for b small. But, of course, time is still $O(\sqrt{n})$.
First improvement (as a general method) is due to Lehman. Observe that if we use auxiliary factors r,s, we may be able to factor a multiple of n. So suppose $n=pq$, (p,q not necessarily prime), and $r/s \sim p/q$, ie, $rq\sim sp$. Consider factorising $4rsn = 4rspq$
$= (rq+sp)^2-(rq-sp)^2$, where $rq-sp$ is 'small'
We can obtain $\left|\frac{r}{s}-\frac{p}{q}\right|<\frac{1}{s^2}$ if r/s is a continued fraction approximation to p/q.
So, $|rq-sp|<q/s$. If we assume $s\sim n^{1/6}$, then there are $n^{1/3}$ choices for (r,s), and each choice leads to $rq-sp<n^{1/3}$.

$2sp=\sqrt{4rsn}\,(1+\varepsilon)$
$2rq=\sqrt{4rsn}\,(1-\varepsilon+\varepsilon^2-\cdots)$
} So, $(sp+rq)=\sqrt{4rsn}\,(1+\frac{1}{2}\varepsilon^2+\cdots)$
$|rq-sp|=\sqrt{4rsn}\cdot\varepsilon$
} So, $\varepsilon\sim\frac{n^{1/3}}{n^{1/6}}\sim\frac{1}{n^{1/3}}$

So $rq+sp$ is in the range $n^{2/3}$ to $n^{2/3}(1+\frac{1}{n^{2/3}})$, ie, # possible values for $rq+sp$ is $O(1)$.
So we get $O(n^{1/3})$ operations, and this is deterministic.

Zero-mod-p methods.

Idea is to compute (mod n) some number f which is $\equiv 0 \bmod p$ (where $p\mid n$), and then obtain p as $\text{hcf}(f,n)$.
Pollard's $(p-1)$-method: Suppose that $p\mid n$ and $p-1$ is smooth, ie, has only 'small' factors.
Assume $p-1$ is B-smooth, ie, all primes $q\mid p-1$ satisfy $q\le B$. Let $C=\prod_{q^e\le B} q^e$.
Then C is a multiple of $p-1$, hence $x^C\equiv 1 \bmod p$, and $\text{hcf}(x^C-1,n)$ should be p.
We form x^C by successively raising x to each power q^e in C, all mod n.
$x\mapsto x^q$ takes $\log q$ steps, so x^C requires $\sum_{q^e\le B}\log(q^e)=\sum_{q\le B}\log q+\sum_{q\le B^{1/2}}\log q+\sum_{q\le B^{1/3}}\log q+\cdots$
Now, $\sum_{q\le B}\log q=\int_1^B \log t\, d\pi(t)=[\log t\cdot\pi(t)]_1^B-\int_1^B\frac{1}{t}\pi(t)\,dt\sim[\log t\cdot\frac{t}{\log t}]_1^B-\int_1^B\frac{dt}{\log t}\sim B$.
So, the cost of the $(p-1)$-method $\sim B+B^{1/2}+B^{1/3}+\cdots\sim B$

Similarly, we can work with $p+1$ by finding d with $\left(\frac{d}{n}\right) = -1$. With probability $\geq 1/2$ we may expect $\left(\frac{d}{p}\right) = -1$. Work in the group of norm 1 elements mod n, ie we choose $\alpha = x + y\sqrt{d} \bmod n$ such that $x^2 - dy^2 \equiv 1 \bmod n$, (in fact, choose x, y first). Then consider C as before, and $\alpha^C - 1$ should reveal p if $p+1$ is B-smooth.
To prevent these methods from working, one often chooses "strong" primes for p, q in RSA numbers, ie $p \pm 1 = (\text{small})(\text{prime})$.

Elliptic Curve Method: Let E be an elliptic curve mod n, and let $p \mid n$. Order of $(E \bmod p)$, ie the group of points of $E(GF(p))$ is $p+1-t_p$, where $|t| \leq 2\sqrt{p}$, and we know every possible t occurs. If order of $E \bmod p$ is B-smooth, take $C = \prod_{q^e < B} q^e$, as before. Choose random point P on $E \bmod n$, and compute $[C]P \bmod n$. (As before, via $P \to [q^{e'}]P \to \dots$). If resulting point is $\equiv 0 \bmod p$, then denominator in coordinates will contain p as a factor. We need to estimate the probability that a randomly chosen E has order mod p which is B-smooth.

(i) Distribution of t for random E. If (A, B) random mod p and E is $Y^2 = X^3 + AX + B$, say. - Unknown.

(ii) if $D = t^2 - 4p$, then the number of isomorphism classes of $E \bmod p$ with $t_p = t$ is $H(D)$, where H is the class number (ie, # classes of binary quadratic forms of discriminant D), and best we can say is that this is $\ll \sqrt{D}$. (One can say more, eg $2^t \mid H$ if D has t prime factors). Recent results of J.F. McKee have shown that these naive remarks underestimate power of method, ie that curves with $p+1 \pm t$ 'smooth' are 'more' likely.

We need to balance B: large $B \to$ plenty of B-smooth curves, small $B \to$ faster computation.
Let $\Psi(x, y) = \#\{n \leq x : p \mid n \Rightarrow p \leq y\} = \#\{y\text{-smooth integers} \leq x\}$

Theorem: Fix u. $\dfrac{\Psi(x, x^{1/u})}{x} \sim u^{-u}$.

We shall see that a better estimate is actually the Dickman-de Bruijn function $\rho(u)$ which satisfies $\rho'(u) = \rho(u-1)$. $\rho(u) \sim u^{-u}$.
So we should choose B such that $B/\Psi(\sqrt{n}, B)$ is minimal. Consider $L[t,c](x) = \exp\left(c(\log x)^t (\log\log x)^{1-t}\right)$
Then, $\frac{1}{x}\Psi(x, L[t,c](x))$ is u^{-u}, where $u = \dfrac{\log x}{\log L[t,c](x)} = \dfrac{\log x}{c(\log x)^t (\log\log x)^{1-t}} = \frac{1}{c}\left(\dfrac{\log x}{\log\log x}\right)^{1-t}$.
So, $u^{-u} = \exp(-u\log u) = \exp\left(-\frac{1}{c}\dfrac{(\log x)^{1-t}}{(\log\log x)^{1-t}}\left[-\log c + (1-t)\log\log x - (1-t)\log\log\log x\right]\right)$
$= \exp\left(\frac{1-t}{c}(\log x)^{1-t}(\log\log x)^t + O(1)\right) = L\left[1-t, \frac{1-t}{c}\right] + o(1)](x)$

Lemma: $y \cdot \dfrac{x}{\Psi(x,y)} \geq L\left[\frac{1}{2}, \sqrt{2} + o(1)\right](x)$, with equality when $y = L\left[\frac{1}{2}, \sqrt{\frac{1}{2}}\right](x)$
Proof: We have just seen that $\dfrac{x}{\Psi(x, x^{1/u})} \sim u^u$, and if y is $L\left[\frac{1}{2}, \theta\right](x)$, then u^u is $L\left[\frac{1}{2}, \frac{-1}{2\theta} + o(1)\right](x)$. Minimum is at $t = 1-t = 1/2$, so want $\theta + \frac{1}{2\theta}$ minimal, ie $\theta = \sqrt{\frac{1}{2}}$

In our case, $\min B/\Psi(\sqrt{n}, B)$ is $L\left[\frac{1}{2}, \sqrt{2}\right](\sqrt{n}) = L\left[\frac{1}{2}, \sqrt{\frac{1}{2}}\right](n)$.
Problems: (i) we have no proof that choosing an elliptic curve at random chooses its order mod p at random.
(ii) no proof that interval $x \pm 2\sqrt{x}$ contains a proportion u^{-u} of $x^{1/u}$-smooth numbers. Indeed, it is not yet proved that there is any $x^{1/u}$-smooth number in this interval.

It has been shown that intervals of length $y^{2+\varepsilon}\sqrt{x}$ contain the 'correct' proportion of y-smooth numbers ($y = x^{1/u}$). McKee's work on problem (i) suggests it is actually favourable. There are results on the proportion of numbers n which can be factorised in given time.

Let $S(x,t,M)$ denote the proportion of $n \le x$ which can be factorised by method M in $\le t$ steps with probability $\ge 1/2$. Knuth and Trabb-Pardo showed: $S(x, x^{1/u}, TD) \sim e^{\gamma}\cdot\frac{1}{u}$, where $\gamma = \lim\left(\sum_{r=1}^{n}\frac{1}{r} - \log n\right) = 0.577\cdots$ is Euler's constant.
Soreuson showed: $S(x, x^{1/u}, p\pm1) \ge \frac{1.9}{u} - \frac{2\log\log x}{u\log x}$, and is $\le \frac{1.8}{u}\cdot\frac{\log\log x}{\log\log\log x}$
Hafner & McCurley showed: $S(x, x^{1/u}, ECM) \ge \frac{1.78}{\log x}\cdot\left(\frac{1}{u}\cdot\frac{\log\log x}{\log x}\right)^{1.199}$
So, ECM is "strictly better" than $p\pm1$. Indeed, ECM found:
1995: P_{44} is C_{99} in $p(19069)$ (ie, 44 digit prime from 99 digit composite of # partitions of 19069).
P_{40} in $2^{1024}+1 = C_{\sim 300}$
1996: P_{47} in C_{155} in $5^{256}+1$. Here, the order of the successful curve was:
$2^6 . 3.5.7.23.997.43237.554573.659723.2220479.2459497.90335969$.

In the last case, Montgomery completed the computation with $Q = [C]P$, $C = \prod_{q^e < B} q^e$, with $B = 3\cdot10^6$.
If $[r]Q = 0$ with $r < 10^{10}$:
Take $H = 10^5$ and compute $Q, 2Q, \ldots, [H]Q$ and $[H]Q, [2H]Q, \ldots, [H^2]Q$ } lists of length H.
$r = \alpha H + \beta$, with $\alpha, \beta < H$, as $r < H^2$. So $\mathcal{O} = [r]Q = [\alpha H]Q + [\beta]Q$.
So, one element of a list = - an element of the other.
Sort each list (by x-coordinate) in time $\sim H\log H$, and look for a match - in time H.
In fact, Montgomery used lists of the form $[2^i.7^j]Q$ and $[3^R.5^L]Q$.
This is Shanks' "Big Step - Little Step" method (for finding the order of a group)

Pollard's Rho Method: Pick a random function f and iterate: $x_1 = f(x_0), \ldots, x_{n+1} = f(x_n)$.
As usual, let $p|N$. If $f: X \to X$ of size x, tail $\sim\sqrt{x}$, head $\sim\sqrt{x}$.  = "rho".
So if $r \sim \sqrt{p}$, then list $x_1, \ldots, x_r$ should have a repeat mod p.
We find the repeat by Floyd's cycle-finding trick. Let $y_n = x_{2n}$, computed by $y_{n+1} = f(f(y_n))$, and wait until $(y_n - x_n, N) = p$. This will happen when # steps $\ge$ length of tail + cycle.

Theorem: Let X be a set of size p and $f: X \to X$ a uniformly random map.
Let $\alpha(x) = \#\{f^i(x),\ i = 0,1,2,\ldots\}$. Then $\mathbb{E}\,\alpha = \sqrt{\frac{\pi}{2}\cdot p}$.
* Indeed, $\mathbb{P}(\alpha < p^{\frac{1}{2}-\varepsilon}$ or $\alpha > p^{\frac{1}{2}+\varepsilon})$ is vanishingly small *.

Lemma: $\log n! = (n+\frac{1}{2})\log n - n + \log 2\pi + B(\frac{1}{12n})$, where $B(\cdot)$ denotes a term less than $(\cdot)$

$\mathbb{P}(\alpha \ge k) = \mathbb{P}($choosing k random distinct numbers from $n) = 1\cdot(1-\frac{1}{n})\cdot(1-\frac{k-1}{n}) = \frac{n!}{(n-k)!\,n^k}$.
$\log\mathbb{P}(\alpha \ge k) = \log n! - \log(n-k)! - k\log n = (n+\frac{1}{2})\log n - n + \log 2\pi + B(\frac{1}{12n}) - (n-k+\frac{1}{2})\log(n-k)$
$+ (n-k) - \log 2\pi - B(\frac{1}{12(n-k)}) - k\log n = (n-k+\frac{1}{2})\log(\frac{n}{n-k}) - k + B(\frac{1}{6(n-k)})$
Let $k = K\sqrt{n}$. Then, $\log\mathbb{P}(\alpha \ge K\sqrt{n}) = -(n-K\sqrt{n}+\frac{1}{2})\log(1-\frac{K}{\sqrt{n}}) - K\sqrt{n} + B(\frac{1}{6(\sqrt{n}-K)\sqrt{n}})$
$= -(n-K\sqrt{n}+\frac{1}{2})(\frac{K}{\sqrt{n}} + \frac{K^2}{2n} + B(\frac{2K^3}{n^{3/2}})) - K\sqrt{n} + B(\frac{1}{6(\sqrt{n}-K)\sqrt{n}}) = -\frac{K^2}{2} + B(\frac{c_\varepsilon}{\sqrt{n}})$, where c_ε is an absolute constant provided $n^{-\varepsilon} < K < n^{\varepsilon}$.

So for $n^{-\varepsilon} < K < n^{\varepsilon}$ we have $\mathbb{P}(\alpha > K\sqrt{n}) = e^{-K^2/2} \times (1 + \text{error})$, error $\to 0$ with n (ie uniformly in K).
Density of α is the derivative of $e^{-K^2/2}$ wrt K, and almost all of probability mass is in this range. So we can estimate $\mathbb{E}(\alpha/\sqrt{n}) = \int_0^\infty e^{-K^2/2} dK = \sqrt{\pi/2}$. So $\mathbb{E}(\alpha) = \sqrt{\pi/2} \cdot \sqrt{n}$.
We conclude that if p is the smallest prime factor of n, Pollard's rho method finds p in average time $\sim \sqrt{\pi/2} \cdot \sqrt{p}$, and almost surely in time $O(\sqrt{p})$

In practice, one uses $f(x) = x^2 + c \bmod n$, for $c \neq 0, -2 \bmod n$. We choose f quadratic rather than linear, for linear gives just a permutation. we must avoid permutations mod n as cycle lengths are large (nearly $\sim n$). Choose $c \neq 0$, as after a certain number of iterations of x^2 we have a permutation on a subset mod n. Also, $x \mapsto x^2 - 2$ is $u \mapsto u^2$ where $x = u + \frac{1}{u}$ (2^{nd} Chebyshev polynomial). There are no more 'bad' quadratic polynomials. (There is a theorem: if $f_m(f_n(x)) = f_{mn}(x)$, then f is a power or a Chebyshev polynomial).

* Theorem (Bach): Choosing c at random mod n gives: $\mathbb{P}(p \text{ emerges in } k \text{ steps}) \geq \frac{1}{p}\left(\frac{k}{2}\right) + O(p^{-3/2})$ *

So choosing c at random and $f(x) = x^2 + c$ means expected time is still $\sim \sqrt{p}$.

Exercise: $x \mapsto x^2 + c$ is a 2-to-1 map. What happens if we take f to be a 'random' 2-to-1 map?

Square-root-of-one methods
These all depend on solving equation $x^2 \equiv 1 \bmod n$ with $x \neq \pm 1$. (or $u^2 \equiv v^2$ with $u \neq \pm v$).
We saw # solutions to $x^2 \equiv 1 \bmod n$ is $2^{w(n)}$, where w = # distinct prime factors of n.
we assume n is known to be composite and not a perfect power (though n could have repeated roots. We know of no faster method of showing n is square free than factorising).
Fermat's method: $n = a^2 - b^2$ } can be seen as solving $a^2 \equiv b^2 \bmod n$.
Lehman: $4rsn = a^2 - b^2$ }
Mention Shanks' quadratic forms method. Expected time $O(n^{1/4})$. if we assume ERH, time is $O(n^{1/5})$

Dixon's Factor Base Method: Use a factor base $\mathcal{B} = \{p < Y\}$. Write down $x \bmod n$ at random, and consider $y = x^2 \bmod n$ (reduced). Test whether y is smooth wrt $\mathcal{B}$, ie composed of p in $\mathcal{B}$.
If so, record $x_i^2 \equiv \prod_j p_j^{e(i,j)} \bmod n$, a smooth relation, and wait till we have more than $|\mathcal{B}|$ relations. Try to solve equation $\prod_i x_i^2 = \prod_i \prod_j p_j^{e(i,j)} = \prod_j p_j^{\sum_i e(i,j)} = \text{square}$, ie want $\sum_i e(i,j) \equiv 0 \bmod 2$, each j.

Example: $n = 84101$, $\mathcal{B} = \{2, 3, 5, 7, 11, 13, 17\}$

x	$x^2 \bmod n$	factors	
12191	14014	$2 \cdot 7^2 \cdot 11 \cdot 13$	
17451	7680	$2^9 \cdot 3 \cdot 5$	} ✓
65308	36750	$2 \cdot 3 \cdot 5^3 \cdot 7^2$	} ✓

So $(17451 \cdot 65308)^2 \equiv (2^5 \cdot 3 \cdot 5^2 \cdot 7)^2 \bmod n$, so $37257^2 \equiv 16800^2 \bmod n$, so $n = 37 \cdot 2273$.

We generated x such that $x^2 \bmod n$ is smooth. Say $x_i^2 = \prod_{q_j} q_j^{e(i,j)}$.
$\prod_{i \in I} x_i^2 = \prod_{i \in I} \prod_{q_j} q_j^{e(i,j)} = \prod_j q_j^{\sum_i e(i,j)}$, where $\sum_i e(i,j) \equiv 0 \bmod 2$, for each j, say $= 2f_j$.
So $(\prod x_i)^2 = (\prod q_j^{f_j})^2$, and with probability $\geq 1/2$ this reveals a factor of n.

Suppose $\mathcal{B}$ consists of primes $\le Y$, and $|\mathcal{B}| = b$, so $b \sim Y/\log Y$. We need at least b smooth relations, since $\{e_i \bmod 2\}$ must be linearly dependent (over GF(2)). Easy to check that if we have $b(1-\varepsilon)$ random vectors in $GF(2)^b$ they are almost certainly independent, whereas if we have $b(1+\varepsilon)$, almost certainly dependent.
The chance that $x_i^2 \bmod n$ is Y-smooth is $\frac{\Psi(n,Y)}{n}$. So, # x_i's required to find b smooth relations is $\sim \frac{n}{\Psi(n,Y)} \cdot b$. Then we have $b \times b$ set of linear equations to solve.
Obvious methods such as Gaussian Elimination solve these in $O(b^3)$ steps. Sophisticated methods reduce this to $O(b^{2+\varepsilon})$.
As usual, put $Y = L[t,c](n)$. Then, optimization shows we need $t = 1/2$, and we take $Y = L[\frac{1}{2}, \frac{1}{2}](n)$ to get overall time of $L[\frac{1}{2}, 2](n)$.

Continued Fraction Method: Replace random x_i with $x_i^2 \bmod n$ about size of n by developing $\sqrt{n}$ (or $\sqrt{kn}$, k a small multiple) as a continued fraction. Then get a sequence of approximations p/q with $|\sqrt{n} - p/q| < 1/q^2$. So $|q\sqrt{n} - p| < 1/q$ and $q\sqrt{n} + p < 2q\sqrt{n} + 1/q$.
Multiplying together gives $|q^2 n - p^2| < 3\sqrt{n}$, say. ie, $p^2 \bmod n < 3\sqrt{n}$.
We obtain a sequence of p such that $p^2 \bmod n$ is of size $\sim \sqrt{n}$, and so is more likely to be smooth. With this, the time is now $L[\frac{1}{2}, 1.23](n)$

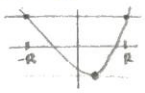
Quadratic Sieve Method: introduces two new ideas. First is to consider $(x + \lfloor\sqrt{n}\rfloor)^2 \bmod n$ for small x.
$(x+\lfloor\sqrt{n}\rfloor)^2 = x^2 - 2x\lfloor\sqrt{n}\rfloor + \lfloor\sqrt{n}\rfloor^2 = x^2 - 2x\sqrt{n} + O(x) + n + O(\sqrt{n})$.
So $(x - \lfloor\sqrt{n}\rfloor)^2 - n = O(x\sqrt{n})$ if $x = O(\sqrt{n})$. So $(x - \lfloor\sqrt{n}\rfloor)^2$ is again of size $x\sqrt{n}$.
Second, and the more important idea, is that values $(x - \lfloor\sqrt{n}\rfloor)^2$ are taken over a consecutive range of x, eg $-R < x < R$, some R. So we have values $Q(x) = x^2 - Ax + B$, where $A = \lfloor\sqrt{n}\rfloor$, $B = \lfloor\sqrt{n}\rfloor^2 - n$, for $-R < x < R$ to test for smoothness
Form an array of cells $C[-R], \ldots, C[R]$ (one for each value of x in range). Idea is to accumulate in $C[x]$ the primes $q \in \mathcal{B}$ which divide $x^2 - Ax + B$. We only trial divide if $C[x]$ is 'full'.
In detail: initially take $C[x] = 0$, for each q in $\mathcal{B}$ add $\log q$ to cells $C[x]$ such that $q \mid Q(x)$. Finally if $C[x]$ contains $\log Q(x)$, we know $Q(x)$ is $\mathcal{B}$-smooth, and proceed to trial division for $Q(x)$.
Given q, cells $C[x]$ with $q \mid Q(x)$ are those $C[x]$ such that $x^2 - Ax + B \equiv 0 \bmod q$, ie such that $x \bmod q \equiv x_1$ or x_2 where x_1, x_2 are roots $x^2 - Ax + B \bmod q$. ie, x we want lie in one of a number $(0, 1, 2)$ arithmetic progressions mod q.
So, # operations is $\frac{2R}{q} \cdot 2$ and $4R \cdot \sum_{q<Y} q^{-1} \sim 4R \log\log Y$. (cf. $2R \cdot \frac{Y}{\log Y}$ by trial division).

Practical Variations.

1. Note $\mathcal{B}$ need only contains primes q with $(\frac{n}{q}) = 1$
2. If $Q(x)$ is not $\mathcal{B}$-smooth then it has factor $r > Y$. So if $C[x] \neq \log Q(x)$ at end, it differs by $> \log Y$. We can compute $\log q$ and $\log Q(x)$ crudely (Indeed, we do not need to compute many values of $\log Q(x)$).
3. Previous remark also helps when $Q(x)$ has repeated factors. It can pay to treat $4, 8, 9, 25, \ldots$ (ie, powers of smalls), as 'primes' q, with, eg, '$\log$' $4 = \log 2$.

So, we took $Q(x) = x^2 + Ax + B$, where $A = -\lfloor \sqrt{n} \rfloor$, $B = A^2 - n$, x in the range $-R, \dots, +R$ ($R \ll \sqrt{n}$).
So $Q(x) \leq R\sqrt{n}$. Find smooth values of $Q(x)$ by sieving: array $C[x]$, $x = -R, \dots, R$. For each $q \in \mathcal{B}$, add $\log q$ into $C[x]$ where $x \equiv x_1$ or $x_2 \bmod q$, the roots of $Q(x) \bmod q$.
$Q(x)$ is $\mathcal{B}$-smooth if $C[x] = \log Q(x)$ afterwards. Indeed, sufficient to have $C[x] > \log Q(x) - \log Y$, the "threshold", where $\mathcal{B} = \{q < Y : \left(\frac{n}{q}\right) = +1\}$. Then, the x for which $Q(x)$ is smooth can be processed as in Dixon's factor method, ie factor $Q(x)$ by Trial Division.

The size of numbers $Q(x)$ involved is $\sim R\sqrt{n}$. So next major improvement is to take multiple polynomials $Q(x)$ of form $ax^2 + bx + c$ with discriminant $b^2 - 4ac = n$. Then, $4a \cdot Q(x) = (2ax + b)^2 - n$, so $4a\,Q(x)$ is a known square mod n. Aim is to take range $x \in \{-R, \dots, R\}$ and many values of (a,b,c), so that $4a \cdot Q(x)$ is as small as possible.
Consider polynomial $ax^2 + bx + c$. Want to maximise $\equiv$ # smooth $Q(x)$, $x \in [-R, R]$. Approximate by minimising $\max_{x \in [-R,R]} |Q(x)|$, and this is done by having minimum (vertex of parabola) near centre of range. So want b small and $Q(\pm R)$ roughly equal to each other, and to $-Q(0)$.



Now, $b^2 - 4ac = n$. We fix a, c by $aR^2 \pm bR + c \cong -c$, ie $aR^2 \pm \cdots -c$. So $a \simeq \frac{\sqrt{n}}{2R}$, $c \simeq \frac{R}{2}\sqrt{n}$.
Then given a (say), b is determined (mod $2a$) by $b^2 \equiv n \bmod 4a$, and $c = \frac{b^2 - n}{4a}$

So we are testing numbers of about size of $c \sim \frac{R}{2}\sqrt{n}$, by R has been divided by $\#(a,b,c)$ we are going to use. So the average size of number $Q(x)$ is smaller, hence more likely to be smooth. Smooth relation must include factorisation of a. Various choices include:
(i) take $a = \alpha^2$, square.
(ii) include a in $\mathcal{B}$.
(iii) take a to be $\mathcal{B}$-smooth.

Remark: If a is smooth then there are several b with $b^2 \equiv n \bmod 2a$. So, same a, different b, we use the same solution to $Q(x) \equiv 0 \bmod n$.

Large prime variation: In this, we look for values of $Q(x)$ which are (Y,Z)-smooth, ie all primes $\leq Z$, and all but maybe one $\leq Y$. We obtain such values by using $\log Q(x) - \log Z$ as threshold, and this gives (Y,Z)-smooth numbers, provided $Y < Z < Y^2$.
Then, trial divide $Q(x)$ by elements of $\mathcal{B} = \{\text{primes} \leq Y\}$, and cofactor is either 1 or a prime $L < Z$.
We then need to eliminate L from the relation. Accumulate smooth relations, until L reappears: $Q(x) = L \cdot (\text{smooth})$, $Q(x') = L \cdot (\text{smooth})$. Then $Q(x)Q(x') = L^2 \cdot (\text{smooth}) = \text{square}$ gives smooth relation.
Next step: double large prime. As before, except we allow $Q(x) = (\text{smooth}) \cdot L_1 \cdot L_2$, where L_1, L_2 are 'large' primes, ie $Y < L_1, L_2 < Z$.
Note: we are faced with auxiliary factorisations. ie, need to know L_1, L_2, given only $L_1 L_2$.
Typically, this would be the EC method, or Pollard's ρ or Jackson's SQUFOF method.

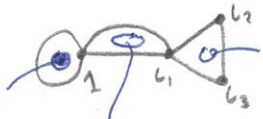
To eliminate large primes, we draw a graph on vertices $\{L\}$ of large primes which occur, together with 1. Each relation gives an edge:

$1 \circ$ - smooth.

$1 \circ\!\!-\!\!- L_1$ - (smooth)$\cdot L_1$

$L_1 \circ\!\!-\!\!- L_2$ - (smooth)$\cdot L_1 \cdot L_2$.

We look for (a basis for) cycles, since each L will appear twice in a cycle.

For example: 

get (smooth) $\times$ L_1L_2, L_1L_3, L_2L_3. product = (smooth). square

get 2 relations, (smooth) L_1, (smooth) L_1 - take product.

MPQS (PP): Sieving can be split up over many processors.
The RSA-129 challenge number was factored in 1993-4 using MPQS-PP over thousands of processors on the Internet with relations accumulated in idle time and collected by e-mail - in ~ 6000 MIPS-years. The message encrypted was "The Magic Words Are Squeamish Ossifrage."

In 1995, Leyland factored a 384-bit number using only idle time on Oxford University computing service CPUs. (~ 116 digits).

Number Field Sieve. (NFS)
Developed by Pollard to factor $F_9 = 2^{2^9}+1$, and used special form of F_9.
Factorisation was completed in 1990.
Idea is to have an algebraic side and a rational side. We express n as $f(m) = n$, where f is a polynomial, and work in $\mathbb{Z}[\alpha]$, α a root of f, and in $\mathbb{Z}/n\mathbb{Z}$.

Let $\varphi: \mathbb{Z}[\alpha] \to \mathbb{Z}/n\mathbb{Z}$ - a ring homomorphism.
$\alpha \mapsto m \bmod n$

Plan to obtain element $x+y\alpha \in \mathbb{Z}[\alpha]$ such that
(i) $x + y\alpha = \xi^2$, $\xi \in \mathbb{Z}[\alpha]$.
(ii) $\varphi(x+y\alpha) = x+ym \bmod n$ is a square z^2.
Then $\varphi(\xi)^2 = z^2$ is a candidate for factoring n. In each case, we build up ξ, z out of "smooth relations"

Norm of an element w = polynomial in α, say $w(\alpha)$ is $\prod_{i=1}^{d} w(\alpha^{(i)})$, where $\alpha^{(i)} = \alpha, \alpha^{(2)}, \ldots, \alpha^{(d)}$ are the roots of f (in $\mathbb{C}$, say). If f and w have integer coefficients, the norm is rational. Indeed, norm of $x+y\alpha$ is $y^d f(x/y)$.
We can test $x+y\alpha$ for smoothness by testing its norm for smoothness (as an integer).

Example: $n = 84101 = 290^2+1$. Put $f(x) = x^2+1$ and $m = 290$. Note f is irreducible and root $\alpha = i$ generates $\mathbb{Z}[i]$, a UFD, with units $\{\pm 1, \pm i\}$.
Let $\mathcal{A} = \{$primes of $\mathbb{Z}[i]$ of norm $\le 17\}$, $\mathcal{B} = \{$primes of $\mathbb{Z} \le 17\}$.
$|x|, |y| < 50$.

x	y	$N(x+yi)$	$x+ym$.
-50	1	$2501 = 41.61$	$240 = 2^4.3.5$
-50	3	$2509 = 13.193$	$820 = 2^2.5.41$
-49	43	$4250 = 2.5^3.17$	12421 = prime
-38	1	$1445 = 5.17^2$	$252 = 2^2.3^2.7$
-22	19	$845 = 5.13^2$	$5488 = 2^4 7^3$.

Factorising in $\mathbb{Z}[i]$, $\quad -38+i = -(2-i)(4-i)^2$

$\quad -22+19i = -(2+i)(3-2i)^2$

So $(-38+i)(-22-19i) = (2-i)^2(3-2i)^2(4-i)^2 = (31-12i)^2$,

and $f(31-12i) = 31-12m = -3449 \equiv$ ~~$2^2 \cdot 3^2 \cdot 7 \cdot 2^4 \cdot 7^3$~~, and this squared is $\equiv 2^2 3^2 . 7 . 2^4 . 7^3 . = 1176^2$.

So hcf $(n, -3449 \pm 1176) = 2273, 37$.

Pollard chose $2.F_9 = 2^{513}+2 = (2^{171})^3+2$ and $f(x) = x^3+2$. Again, $\mathbb{Z}[\alpha]$ is a PID.

These are examples of Special NFS. [ie $f(x)$ is particularly convenient].

Sieving comes in search for $x+y\alpha$ which are smooth. Fix y, say, then Norm $(x+y\alpha)$ is a polynomial in x, say $P_y(x)$. We form an array $C[x]$ as before and 'post' $\log q$ into cells for which $P_y(x) \equiv 0 \bmod q$, ie, $x \equiv$ root of $P_y \bmod q$.

Size of numbers involved:

$*\text{Norm}(x+y\alpha) \sim R^d . f(R)$, where R is range of x, y.

$x+ym \sim Rm$

So aim to get coefficients of f and size of root m of $f \bmod n$ small.

It is easy to see that two numbers of size y, say, are more likely to be smooth than one of size y^2.

A careful analysis suggests that the General NFS should take time $L[\frac{1}{2}, 1.92]$.

Old method: trial division: $L[1, \frac{1}{2}]$

Lehmen : $L[1, \frac{1}{3}]$

EC, QS : $L[\frac{1}{2}, c]$

NFS : $L[\frac{1}{3}, 1.92]$.

Ideal would be $L[0, c]$, ie $(\log N)^c$, ie polynomial time.

Sample Results.

	Method	Time (MIPS-years)
RSA -100	MPQS	7
C_{105} - factor of $3^{367}-1$	SNFS	~100
RSA - 110	MPQS	800
Blacknet: PGP-116	MPQS	400
C_{116} - factor of $7^{194}+1$	MPQS	?
RSA - 120	MPQS	835
RSA - 129	MPQS	4-6,000
RSA - 130.	GNFS	~10.

Conclude GNFS is in practice the most powerful method for ≥ 120 digits, and extreme limit today ~ 130 - 140 digits. Experiments suggests 10 digits = 10-fold increase in time.

Shor proves that a quantum computer can factor in time $L[0,2]$.

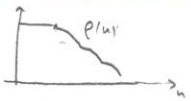
"STOP PRESS! $2^{1398269}-1$ is prime. (23/11/96)."

Smooth Numbers.

Let $\Psi(x,y) = \#\{n \le x : p|n \Rightarrow p \le y\}$ = # y-smooth integers less than x.
Buchstab recurrence: $\Psi(x,y) = \Psi(x,z) + \sum_{z<p\le y} \Psi(x/p, p)$ for $y > \sqrt{z}$.
Putting $u = \frac{\log x}{\log y}$ (so $y = x^{1/u}$), use induction on $\lfloor u \rfloor$

If $u<1$, so $\lfloor u \rfloor = 0$, then $\Psi(x,y) = \lfloor x \rfloor$.
For $1 \le \lfloor u \rfloor \le 2$, put $z = x$: $\Psi(x,y) = \lfloor x \rfloor - \sum_{y<p\le x} \lfloor \frac{x}{p} \rfloor \sim x - \sum_{y<p\le x} \frac{x}{p} = x\left(1 - \sum_{y<p\le x} \frac{1}{p}\right)$
Now $\sum_{p\le t} \frac{1}{p} \sim \log\log t$. So $\sum_{y<p\le x} \frac{1}{p} \sim \log\log x - \log\log y = \log\left(\frac{\log x}{\log y}\right) = \log u$.
So $\Psi(x,y) \sim x(1-\log u)$, (using a form of PNT with a good error).

Iterating: $\Psi(x,y) \sim x\rho(u)$, where $\rho(u) = \rho(k) - \int_k^u \rho(v-1)\frac{dv}{v}$, $k = \lfloor u \rfloor$.
Hence ρ is the solution to the differential-delay equation: $\rho'(u) = -\frac{\rho(u-1)}{u}$,
for $u>1$, and $\rho(u) = 1$ for $0<u<1$



It is well-known that $\rho(u)$ is asymptotic to u^{-u}.
So we expect that $\frac{\Psi(x,x^{1/u})}{x} \sim u^{-u}$. Aim to prove this directly.

An easy calculation shows that $\frac{\Psi(x,x^{1/u})}{x} \gtrsim u^{-3u}$

Proof: Wlog, $u^{3u} > x$, and $u > (\log x)^{3/8}$
(die get $\Psi(x,x^{1/u}) \gtrsim (?<1)$ & ?!. — otherwise count powers of 2.

Suppose $c \le x$ and $x^{1/u} > c^3$. $\pi(x^{1/u}) > \frac{1}{2}\cdot\frac{x^{1/u}}{\log x^{1/u}} = \frac{1}{2}\frac{u x^{1/u}}{\log x}$ for $c > 10^6$.
Write $u = k+\theta$, where $k = \lfloor u \rfloor$.
$\Psi(x,x^{1/u}) \gtrsim \frac{\pi(x^{1/u})^k \cdot \pi(x^{\theta/u})}{(k+1)!}$, counting $n = p_0\cdot p_k$, with $p_0 < x^{\theta/u}$, $p_1,\dots,p_k < x^{1/u}$

$\gtrsim \left(\frac{u x^{1/u}}{2\log x}\right)^k \cdot \left(\frac{x^{\theta/u}}{2\log x}\right) / (k+1)! \gtrsim \frac{(\text{same})}{u^k}$ (Stirling)

$= \frac{(x^{\frac{1}{u}})^{k+\theta}}{(2\log x)^{k+1}} = \frac{x}{(2\log x)^{k+1}} = x\exp\left(-(k+1)\log(2\log x)\right)$

$\gtrsim x\exp\left(-(u+1)[\log 2 + \log\log x]\right)$ (as $u > (\log x)^{3/8}$) $\gtrsim x\exp\left(-(u+1)\left[\log 2 + \tfrac{8}{3}\log u\right]\right)$

~~$\gtrsim x\exp(-(u+1)[\log 2 + \frac{8}{3}\log x]$~~ $\gtrsim x\exp(-u.3\log u)$

So $\frac{\Psi(x,x^{1/u})}{x} \gtrsim u^{-3u}$

Theorem: Fix $\varepsilon > 0$. If $(\log x)^{\varepsilon} < \log y < (\log x)^{1-\varepsilon}$, then $\frac{\Psi(x,y)}{x} = \exp(-(1+o(1))\, u \log u)$ uniformly as $x \to \infty$, where $u = \log x / \log y$.
Ie, $\frac{\log(\frac{1}{x}\Psi(x,y))}{\log u^{-u}} \to 1$ as $x \to \infty$, uniformly in u.

Proof: in two parts: upper and lower bounds.

Upper: $\Psi(x,y) = \sum_{\substack{n \le x \\ P(n) \le y}} 1$ ($P(n)$ = largest prime in n). U.b. valid for $(\log x)^{2+\varepsilon} < y < x^{\varepsilon}$

$\le \sum_{\substack{n \le x \\ P(n) \le y}} \left(\frac{n}{x}\right)^{-c}$, some $c < 1$

$= x^c \cdot \sum_{\substack{n \le x \\ P(n) \le y}} n^{-c} \le x^c \cdot \sum_{P(n) \le y} n^{-c} = x^c \cdot \prod_{p \le y} (1-p^{-c})^{-1}$, as before.

We choose c later (close to 1). Choose x sufficiently large that $c > \frac{1}{2} + \varepsilon$
$\log \prod_{p \le y} (1-p^{-c})^{-1} = -\sum_{p \le y} \log(1-p^{-c}) = \sum_{p \le y} p^{-c} + O(1)$, where $O(1)$ depends only on ε (*)
if we take such c.
This is because $|\log(1-t) - t| \le \frac{t^2}{2}$ for $|t| < 1/2$.
So, (tail in (*)) $\le \frac{1}{2} \sum_{p \le y} p^{-2c} \le \frac{1}{2} \sum_{n} n^{-1-2\varepsilon} = O_{\varepsilon}(1)$

Now, $\sum_{p \le y} p^{-c} = \int_1^y t^{-c}\, d\pi(t) = \left[t^{-c}\pi(t)\right]_1^y + c\int_1^y t^{-c-1}\pi(t)\,dt$.
Use PNT in form $\pi(t) = \mathrm{Li}(t) + o(t/\log t)$ to explain why we take $c = 1 - \frac{\log u}{\log y}$.

$\sum_{p \le y} p^{-c} = \mathrm{Li}(y^{1-c})\left(1 + O\left(\frac{1}{\log y}\right)\right) + O(\log|1-c|)$
Optimal value of c will be when $c\log x - \mathrm{Li}(y^{1-c})$ is minimised.
Differentiating, we want c to satisfy $y^{1-c} = (1-c)\log x$ and our choice of c is close to this.
So pick $c = 1 - \frac{\log u}{\log y}$ and substitute in $\Psi(x,y) \le x^c \exp\left(\sum_{p \le y} p^{-c} + O(1)\right)$, to get: $\Psi(x,y) \le x \cdot \exp(-u\log u + o(u))$

So $\log \frac{\Psi(x,y)}{x} \le -u\log u\left(1 + o\left(\frac{1}{\log u}\right)\right)$, hence upper bound.

Lower: Argument is a two-step version of previous u^{-3u} argument.
Fix x, y, u. Let $k = \lfloor u \rfloor$, $\mathcal{M}$ = set of integers m composed of k primes all in range $\left(y^{1-1/\log u}, y\right]$.
$z = y^{1-1/\log u}$ and $w = y^{1-2/\log u}$.
So if $m \in \mathcal{M}$, we have $z^k < m \le y^k \le y^u = x$.

Buchstab relation. $\Psi(x,y) \ge \sum_{m \in \mathcal{M}} \Psi\left(\frac{x}{m}, z\right)$. Indeed, if $mj \le x$ with $m \in \mathcal{M}$, j being z-smooth,
Then mj is y-smooth and $mj < x$
Different pairs (m,j) give different products mj. Fix an $m \in \mathcal{M}$.
Now take $w = y^{1-2/\log u}$ and let $u_0 = \frac{\log(x/m)}{\log z}$.

As before, we have $\Psi\left(\frac{x}{m}, z\right) \ge \sum_{j \in J} \Psi\left(\frac{x}{mj}, w\right)$, where J is the "new $\mathcal{M}$", ie J = set of numbers which are a product of $k_0 = \lfloor u_0 \rfloor$ primes, all in range $(w, z]$.

Now, $\frac{x/m}{j} \geq \frac{x/m}{z^{k_0}}$ (as $j \leq z^{k_0}$). But $x/m = z^{u_0}$, by definition of u_0,
So $\frac{x/m}{j} \geq z^{f_0}$, where $f_0 = \{u_0\}$ = fractional part of u_0.

$\psi(\frac{x}{m_j}, w) \geq \psi(z^{f_0}, w) \geq \lfloor z^{f_0} \rfloor - \sum_{w \leq p < z} \lfloor \frac{z^{f_0}}{p} \rfloor \geq (z^{f_0}+1)(1 - \sum_{w \leq p < z} 1/p)$
But $\sum_{w \leq p < z} \frac{1}{p} \sim \log\log z - \log\log w$.

Now, $\log\log z = \log\log y^{1 - 1/\log u} = \log\left((1 - \frac{1}{\log u})\log y\right) = \log(1 - \frac{1}{\log u}) + \log\log y$.
Similarly, $\log\log w = \log(1 - \frac{2}{\log u}) + \log\log y$.
So, $\log\log z - \log\log w = \log\left(\frac{\log u - 1}{\log u - 2}\right) \to 0$.

So, $\psi(\frac{x}{m_j}, w) > \frac{1}{2} z^{f_0}$ for x sufficiently large. (depending only on ε).

So, $\psi(\frac{x}{m}, z) > \frac{1}{2} \sum_{j \in J} z^{f_0} = \frac{1}{2} z^{f_0} \cdot |J|$
$|J| \geq \frac{1}{k_0!} (\pi(z) - \pi(w))^{k_0}$

$\pi(z) \sim \frac{z}{\log z} = \frac{y^{1 - 1/\log u}}{(1 - \frac{1}{\log u})\log y}$, $\pi(w) \sim \frac{w}{\log w} = \frac{y^{1 - 2/\log u}}{(1 - \frac{2}{\log x})\log y} < \frac{1}{2}\pi(z)$ for x sufficiently large.

So $|J| \geq \frac{1}{k_0!} \cdot \left(\frac{1}{2} \cdot \frac{z}{\log z}\right)^{k_0}$.

So $\psi(\frac{x}{m}, z) \geq \frac{\frac{1}{2} z^{f_0} z^{k_0}}{(2k_0 \log z)^{k_0}} = \frac{z^{u_0}}{2(2k_0 \log z)^{k_0}} = \frac{x/m}{2(2k_0 \log z)^{k_0}}$, by definition of u_0.

So far: $\psi(x, y) \rightsquigarrow \sum_m \psi(\frac{x}{m}, z)$. Need to eliminate k_0 and substitute.

Now, $m \geq z^k$, so $u_0 = \frac{\log x - \log m}{\log z} \leq \frac{\log x}{\log z} - k \leq \frac{u \log u}{\log u - 1} - u + 1$

$= \frac{u}{\log u - 1} + 1$

Now, $\log\log z \leq \log\log y = O(\log u)$, with O depending on ε,
as $\varepsilon \log\log x \leq \log\log y \leq (1-\varepsilon)\log\log x$, and $\log u = \log\left(\frac{\log x}{\log y}\right) = \log\log x - \log\log y$.
$\geq \frac{\log\log y}{1-\varepsilon} - \log\log y = \log\log y \left(\frac{1}{1-\varepsilon} - 1\right)$

$u_0(m) \leq \frac{u}{\log u - 1} + 1$. Claim that $\left((u_0(m)+1) \cdot 2\log z\right)^{u_0(m)} \leq e^{Ku}$, with K dependent only on ε. (in particular, independent of m)

$\log\left((u_0+1) \cdot 2\log z\right)^{u_0} = u_0\left(\log(u_0+1) + \log 2 + \log\log z\right)$

$\leq \left(\frac{u}{\log u - 1} + 1\right)\left(\log\left(\frac{u}{\log u - 1} + 2\right) + \log 2 + C \cdot \log u\right)$

$\leq (u + \log u - 1)(\log u - \log\log u + \log 4 + C\log u) / (\log u - 1)$
$\leq Ku$, for x (and hence u) sufficiently large. (depending on ε).

So $\psi(\frac{x}{m}, z) \geq \frac{1}{2}\frac{x}{m} e^{-Ku}$, and so $\psi(x,y) \geq \frac{1}{2}\sum_{m \in M} \frac{x}{m} e^{-Ku} = \frac{1}{2} x e^{-Ku} \sum_{m \in M} \frac{1}{m}$

$\frac{\psi(x,y)}{x} \geq \frac{\frac{1}{2} e^{-Ku}}{k!} \left(\sum_{z < p \leq y} \frac{1}{p}\right)^k$. Now, $\sum_{z < p \leq y} \frac{1}{p} \sim \log\log y - \log\log z = \frac{1}{\log u}$

$\frac{\psi(x,y)}{x} \geq \exp\left(-Ku + \log 1/2 - u\log u - u\log\log u\right)$

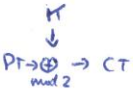
So $\log \frac{\psi(x,y)}{x} \geq$ a function $\sim -u\log u$. So done.

4. Cryptography

Cryptographic systems - Engineering, Human Factors.
|
Protocols - Special reasoning, Probability.
|
Elements - Number Theory, Group Theory.

Needs: for elements to produce:
- secrecy: $A \xrightarrow{m} B$, only the intended recipient can read M.
- authenticity: Only the intended sender can transmit M.
- non-repudiation: A cannot deny sending M.
- integrity: M cannot be changed to M' in transit.
- commitment: B cannot read M until later, but A cannot change it.

Secret-key or symmetric cryptography: A, B share a secret K and enciphering and deciphering require same secret K.
Eg: Vernan or one-time-pad cipher:



Public Key Cryptography: Enciphering and deciphering use different keys, E, D say. The security of D is obtained by intractibility of a problem, say factorisation. So E could be made public, yet it remains infeasible to compute D without some secret "trap door" information.

RSA system: $N = pq$, p, q secret. $DE = 1 \bmod (p-1)(q-1)$. Publish E, N (not D, p, q)
Anyone can form $M^E \bmod N$; only possessor of D can compute $(M^E)^D \bmod N$, which is $\equiv M$, as $DE \equiv 1 \ (\varphi(N))$.

Proposition: Obtaining D is (RP) equivalent to factoring N.
Proof: Factoring N ⇒ obtaining D. (Euclid).
Suppose we have D, so we know $DE \equiv 1 \bmod \varphi(N)$.
Write $DE - 1 = 2^r \cdot s$, $r \geq 1$, s odd. Take b mod N at random and form a

Miller-Rabin sequence, b^s, b^{2s}, b^{4s}, ..., $b^{2^r s}$. Last term is $\equiv 1 \bmod N$ as $2^r \cdot s = DE - 1 \equiv 0 \bmod \varphi(N)$. With probability $\geq 1/2$, power of 2 in orders of $b \bmod p$, $b \bmod q$ are different. If so the first occurrence of $1 \bmod N$ is preceded by $u \not\equiv \pm 1 \bmod N$, but $u^2 \equiv 1$, so N is factored.

Note: Not the same as saying that finding M is equivalent to factoring.

Håstad observed that if that if $E = 3$, say, & the same message is encoded for 3 people, $M^3 \bmod N_1$, $\bmod N_2$, $\bmod N_3$, then by CRT we know $M^3 \bmod N_1 N_2 N_3$, but if $M < N_1, N_2, N_3$, this is M^3, and we've done.

Theorem: Finding one bit of M from $M^3 \pmod N$ is (RP), equivalent to finding M.

Other problem used to protect the secret key is discrete logarithm.
Fix prime p, and g in multiplicative group. Given $g^x \bmod p$, how to find x?
It appears that solving discrete logs mod p is about as hard as factoring n of the same size as p. (Indeed, method used is the same, ie NFS).

Diffie-Hellman key exchange. A, B with to agree on a common secret.
Agree on g mod p. A chooses α at random, B chooses β at random.
They send simultaneously: $A \xrightarrow{g^\alpha} B$
$A \xleftarrow{g^\beta} B$.
A forms $(g^\beta)^\alpha$, B forms $(g^\alpha)^\beta$. So they share a common secret $g^{\alpha\beta} = g^{\beta\alpha}$.
Only known way to obtain $g^{\alpha\beta}$ from g^α, g^β and g is to solve the discrete logarithms for α, β. Maurer recently showed this is the only way, given some conditions on p.

Digital signature
Need hash function, $h(M)$ which is hard to invert. (ie, given h, it's hard to find any M such that $h(M) = h$).
Sign an RSA message as follows: A forms $\left(M, h(M)\right)^{D_A} \bmod N_A)^{E_B} \bmod N_B = X$.
B receives X and forms $(X^{D_B} \bmod N_B)^{E_A} \bmod N_A = M, h(M)$. If so, accepts it.

Digital Signature Architecture.
Choose prime p, let $q \mid p-1$ and g mod p have order q (prime 160 bits).
To sign M, choose k at random, and form $r = g^k \bmod p$, and $s = \frac{h + xr}{k} \bmod q$, where $h = h(M)$. (r,s) is the signature.
Check $g^{h/s} \cdot y^{r/s} = r$, where $y = g^x$ is public, x is secret.

Sun NFS('Network File System'!) uses p of 192 bits and $g = 3$ of order $q = \frac{p-1}{2}$.
As before, x secret, g^x public each machine. Odlyzko took $k[\sqrt{-2}]$ where $k = GF(p)$ and formed equations of the form:

$x+y\sqrt{-2}$ smooth in $\mathbb{Z}[\sqrt{-2}]$.
$x+yd$ smooth in $\mathbb{Z}$, $d^2 \equiv -2 \bmod p$.
where $x+yd$ = either g^u } many u
or $(g^x)^u$ }

we get $g^{u_i} \equiv \pi$ primes in $\mathbb{Z}[\sqrt{-2}] \equiv \pi$ primes in $\mathbb{Z}$, $(g^x)^{u_i} \equiv$ same.
Multiply together. Get $g^{u_1} = (g^x)^{u_2}$, solving equations mod q.
Ie, we have $x \equiv u_1/u_2 \bmod q$.