Computational Number Theory

R G E Pinch
Department of Pure Mathematics and
Mathematical Statistics
University of Cambridge

October 1996

Primality tests

We shall be interested in testing a given integer N for primality. We feel free to assume that N is odd. The tests we consider will return one of three possible results, `prime`, `composite` or `probably prime`. The word "probably" in the last will be made precise in context, but you should think of a this result being correct for 'most' numbers. Some tests will also return a *witness*, or *certificate*, which enables the reader to reproduce or verify the result of the test quickly. A number for which a test returns `probably prime` is a *probable prime* for, or *passes*, that test: if the number is in fact composite, it will be a *pseudo-prime.*

We let the *measure* or *length* $\ell(N)$, be the number of bits in the base 2 expansion of N. A test will be *polynomial time* if the time taken to perform the test is bounded above by a polynomial in $\ell(N)$, and *exponential time* if bounded by a polynomial in N.

We illustrate some of these ideas by considering the first and most obvious test, *trial division.* Given N, we test whether N is divisible by $t = 2, 3, \ldots$ up to a limit, initially $N-1$ but after an instant's thought $\sqrt{N}$. The time taken to return a result can be up to $\sqrt{N}$ if N is indeed prime, or $\pi\left(\sqrt{N}\right) \sim \dfrac{\sqrt{N}}{\log N}$ if t runs through a previously computed list of primes: so the test is exponential and not polynomial time. When a result is returned, it is either `composite` with a *witness* t or `prime` with no witness. If I give you the witness t to the result `composite`, you can verify the result in polynomial time by long division — otherwise you have to take my word for the answer or repeat the calculation all over again.

The *Fermat test* is based on Fermat's "Little" Theorem, that if $b \not\equiv 0 \bmod p$ then $b^{p-1} \equiv 1 \bmod p$. Given N we choose a *base* b, either systematically or at random modulo N. If $\mathrm{hcf}(b, N) \neq 1$ then we have a factor of N and return `composite` with witness b. Otherwise we compute $b^{N-1} \bmod N$. If this is not 1 mod N return `composite` with witness b: otherwise return `probably prime`.

The time required for this is controlled by the time required to perform the exponentiation modulo N. By using a divide-and-conquer method, this requires $\ell(N)$ multiplications modulo N and is polynomial time, since an l-bit multiplication can be performed in $O(n^2)$ elementary operations †.

The result `probably prime` can be given even if N is composite. If we consider the base $b = 2$, then we have $2^{340} \equiv 1 \bmod 341$ but $341 = 11 \times 31$ is composite, so that 341 is an example of a Fermat pseudoprime (in fact the smallest). We can see this quickly by noting that $2^{10} \equiv 1 \bmod 11$ by Fermat's little theorem and $2^5 = 31 \equiv 1 \bmod 31$. However, $3^{340} \equiv 56 \bmod 341$ and so a further application of the test correctly returns `composite`.

The force of the word "probably" can be appreciated by first considering the probability that the test returns the answer `probably prime` for given composite N. The set of b for which $b^{N-1} \equiv 1 \bmod N$ forms a subgroup of the multiplicative group modulo N, and so the probability of choosing a base which gives a false return is the index of this subgroup: we denote this proportion by $W(N)$. Unfortunately it is possible to find N with the property that *all* bases prime to N incorrectly return `probably`

† Faster using an advanced algorithm such as FFT.

prime. Such numbers are *absolute* Fermat pseudoprimes, also called *Carmichael numbers.* If N is a Carmichael number, then it will only be revealed as composite by the Fermat test with a base which has a factor in common with N: so for Carmichael numbers, the Fermat test is no better than trial division at returning the correct answer. If N is not a Carmichael number then $W(N)$ will be at most $\frac{1}{2}$.

Proposition

A number N is a Carmichael number if and only if N is composite, squarefree and $p-1$ divides $N-1$ for every prime p dividing N.

Proof: Suppose that N is composite. Clearly N is a Carmichael number iff the exponent $\lambda(N)$ divides $N-1$. If N has a repeated prime factor p then $p \mid \lambda(N)$: so a Carmichael number must be square-free. But if N is square-free, say the product of distinct prime factors p_i then $\lambda(N) = \operatorname{lcm}\{p_i\}$ and so $\lambda(N) \mid N-1$ iff each $p_i - 1$ divides $N-1$. ■

Corollary

A Carmichael number has at least three prime divisors.

Proof: Suppose that $N = pq$ is a Carmichael number with p, q distinct prime factors, $p < q$. Then $q-1 \mid N-1 = pq-1 = (q-1)p+p-1$. So $q-1 \mid p-1$: but $q-1 > p-1$, a contradiction. ■

The smallest Carmichael number is $561 = 3 \times 11 \times 17$. It was recently established that there are infinitely many Carmichael numbers: indeed, $C(X)$, the number of Carmichael numbers less than X is at least $X^{2/7}$ for sufficiently large X. In the other direction, it can be shown that for any $\epsilon > 0$,

$$C(X) \leq X \exp\left(-(1-\epsilon)\left(\frac{\log X \log\log\log X}{\log\log X}\right)\right)$$

for all sufficiently large X.

We give the number of Carmichael numbers up to X for X up to 10^{16}.

X	$\pi(X)$	$C(X)$
10^3	168	1
10^4	1229	7
10^5	9592	16
10^6	78498	43
10^7	664579	105
10^8	5761455	255
10^9	50847534	646
10^{10}	455052511	1547
10^{11}	4118054813	3605
10^{12}	37607912018	8241
10^{13}	346065536839	19279
10^{14}	3204941750802	44706
10^{15}	29844570422669	105212
10^{16}	279238341033925	246683

We defined $W(N)$ to be the probability of a false return of `probably prime` from the Fermat test: that is, the proportion of bases b prime to N satisfying the condition $b^{N-1} \equiv 1 \bmod N$.

Proposition

The probability $W(N)$ of the Fermat test returning `probably prime` *for N on a random base prime to N is*

$$W(N) = \frac{1}{\phi(N)} \prod_{p|N} \mathrm{hcf}(p-1, N-1)$$

Proof: Let N have factorisation $N = \prod_i p_i^{a_i}$. By the Chinese Remainder Theorem, the number of solutions to the equation $b^{N-1} \equiv 1 \bmod N$ is the product of the number of solutions to the congruences $b^{N-1} \equiv 1 \bmod p_i^{a_i}$. For each such p_i, the multiplicative group modulo $p_i^{a_i}$ is cyclic of order $\phi(p_i^{a_i}) = p_i^{a_i-1}(p_i - 1)$, so the number of elements of order dividing $N-1$ is just $\mathrm{hcf}(N-1, p_i^{a_i-1}(p_i-1))$. Since p_i divides N, $N-1$ is prime to $p_i^{a_i-1}$ and the number of solutions in the multiplicative group modulo $p_i^{a_i}$ is $\mathrm{hcf}(N-1, p_i-1)$. Dividing by $\phi(p_i^{a_i})$ and taking the product, the result follows. ■

Our first improvement on the Fermat test is obtained by noting that if N is a prime then the equation $X^2 \equiv 1 \bmod N$ has only the two solutions $X \equiv \pm 1 \bmod N$, whereas if N has more than one prime factor then the equation has at least four solutions (if p, q divide N then the equations $X \equiv \pm 1 \bmod p$ and $X \equiv \pm 1 \bmod q$ can be solved independently). We define the *Euler test* † by modifying the Fermat test to require that $b^{\frac{N-1}{2}} \equiv \pm 1 \bmod N$.

This test certainly includes the Fermat test, and is slightly faster. It is also strictly stronger, for $2^{644} \equiv 1 \bmod 645$, while $2^{322} \equiv 259$, so that $645 = 3 \times 5 \times 43$ is a pseudoprime for the Fermat test base 2, but not for the Euler test. We have $2^{322} \equiv 1 \bmod 129$ and $2^{322} \equiv -1 \bmod 5$.

Unfortunately, this strengthening does not obviate the possibility of absolute pseudoprimes. For example, $N = 1729 = 7 \times 13 \times 19$ has the property that if b is prime to N then $b^{\frac{N-1}{2}} \equiv 1 \bmod N$, so that N is an absolute Euler pseudoprime.

We can further strengthen the Euler test by identifying the sign ± 1. If p is prime, then $b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right) \bmod p$ where the Legendre symbol $\left(\frac{b}{p}\right)$ is $+1$ if b is a quadratic residue of p, -1 is b is a quadratic non-residue and 0 if $p \mid b$.

We define the *Jacobi symbol* $\left(\frac{a}{N}\right)$ for odd positive $N = \prod_i p_i^{a_i}$ by

$$\left(\frac{a}{N}\right) = \prod_i \left(\frac{a}{p_i}\right)^{a_i}. \qquad J1$$

We immediately see that

$$\left(\frac{a}{N}\right) = \left(\frac{a \bmod N}{N}\right), \qquad J2$$

† Terminology varies

and

$$\left(\frac{a}{MN}\right) = \left(\frac{a}{M}\right)\left(\frac{a}{N}\right). \qquad J3$$

From the properties of the Legendre symbol we obtain

$$\left(\frac{ab}{N}\right) = \left(\frac{a}{N}\right)\left(\frac{b}{N}\right), \qquad J4$$

$$\left(\frac{-1}{N}\right) = (-1)^{\frac{N-1}{2}}, \qquad J5$$

$$\left(\frac{2}{N}\right) = (-1)^{\frac{N^2-1}{8}}, \qquad J6$$

and, if M is odd and positive,

$$\left(\frac{M}{N}\right)\left(\frac{N}{M}\right) = (-1)^{\frac{(M-1)(N-1)}{4}}, \qquad J7$$

the last being the law of quadratic reciprocity. These formulae make it possible to obtain $\left(\frac{b}{N}\right)$ without needing to know the factorisation of N. Application of J1 ensures that we may take $0 \leq b < N$, and if b is even, we can extract the power of two in b by J6 and J4. Since b is now positive and odd then J7 can be applied to reduce the computation to that of $\left(\frac{N}{b}\right)$. The computation is very similar to that of the highest common factor of b and N by Euclid's algorithm, with some extra care taken to keep track of the signs. In particular, the computation of the Jacobi symbol can be performed in polynomial time.

The *Euler–Jacobi* test extends the Euler test by requiring that $b^{\frac{N-1}{2}} \equiv \left(\frac{b}{N}\right) \bmod N$. It is again a polynomial time test.

The Euler–Jacobi test is stronger again than the Euler test. Considering 341 tested base 2 we find that $2^{170} \equiv 1 \bmod 341$, so that 341 passes the Euler test base 2, but $\left(\frac{2}{341}\right) = -1$, so that 341 fails the Euler–Jacobi test.

Indeed, we have finally achieved a test with no absolute pseudoprimes.

Proposition

If N is composite, the probability that N will pass the Euler–Jacobi test with a randomly chosen base modulo N is at most $\frac{1}{2}$.

Proof: If N is not a Carmichael number then from the discussion above the result is already true for the Fermat test, which is included in the Euler–Jacobi test. So we may suppose that N is a Carmichael number: that is, N is square-free and if $p \mid N$ then $p - 1 \mid N - 1$.

The bases b which satisfy $b^{\frac{N-1}{2}} \equiv \pm 1 \bmod N$ form a subgroup of the multiplicative group modulo N. It is sufficient to show that this subgroup is not the whole group, which implies that it has index at least 2, and so it is in turn sufficient to exhibit a

base b for which N fails the Euler–Jacobi test. We consider two cases according to the power of 2 which divides $N-1$ and show that in each case there is such a base.

Case 1. Suppose that 2^r is the exact power of 2 dividing $N-1$ and that 2^r divides $p_i - 1$ for every p_i dividing N. Let d be the number of distinct prime factors of N and put define $t_i = 0$ or 1 by $p_i \equiv 1 + t_i 2^r \bmod 2^{r+1}$. We have

$$N \equiv \prod_{i=1}^{d} 1 + t_i 2^r \equiv 1 + T2^r \bmod 2^{r+1}$$

where $T = \sum_i t_i$. Since T is odd, at least one of the t_i must be 1, say t_j: so 2^r is the exact power of 2 in $p_j - 1$. By the Chinese remainder theorem there is an b which is a quadratic non-residue of the prime p_j and which satisfies $b \equiv 1 \bmod p_i$ for $i \neq j$. Then $b^{\frac{p_j-1}{2}} \equiv -1 \bmod p_j$ and $b^{\frac{p_i-1}{2}} \equiv +1 \bmod p_i$ for $i \neq j$. Now $N-1$ is an odd multiple of $p_j - 1$, so that $b^{\frac{N-1}{2}} \equiv -1 \bmod p_j$, and $b^{\frac{N-1}{2}} \equiv +1 \bmod p_i$ for $i \neq j$, which means that that $b^{\frac{N-1}{2}} \not\equiv \pm 1 \bmod N$ and N fails the Euler test base b.

Case 2. Suppose that $2^r \mid N-1$ but 2^r does not divide $p-1$ for some p dividing N. As before, we take b to be a quadratic non-residue of the prime p and $\equiv 1 \bmod q$ for every other q dividing N. We have $b^{\frac{p-1}{2}} \equiv -1 \bmod p$. Since $N-1$ is an even multiple of $p-1$, $b^{\frac{N-1}{2}} \equiv +1 \bmod p$. Hence if N passes the Euler test base b, it must do so with $b^{\frac{N-1}{2}} \equiv +1 \bmod N$. But the Jacobi symbol $\left(\frac{b}{N}\right) = \prod \left(\frac{b}{p_i}\right) = -1$. So $b^{\frac{N-1}{2}} \not\equiv \left(\frac{b}{N}\right) \bmod p$ and N fails the Euler–Jacobi test base b. ■

Corollary

The question "Is N composite" can be answered in random polynomial time. ■

We can strengthen the Euler test in another direction by a further exploitation of the observation that 1 has only two square roots with respect to a prime modulus. The resulting test is the *strong*, or *Miller–Rabin* test. Let $N - 1 = 2^r s$ where s is odd. For a base b, consider the sequence, formed by repeated squaring,

$$b^s, b^{2s}, \ldots, b^{2^{r-1}s} = b^{\frac{N-1}{2}}, b^{2^r s} = b^{N-1} \bmod N.$$

The strong test returns `probably prime` if this sequence either starts $+1 \bmod N$ or ends $\ldots, -1, +1, +1, \ldots \bmod N$. We see immediately that this test includes the Fermat and Euler tests. It is not obvious that it includes the Euler–Jacobi refinement of the Euler test, but we shall see later that this is indeed the case. The strong test can be perfomed in polynomial time.

Once again it is possible for the strong test to return the answer `probably prime` on composite numbers: for example, for $N = 4033 = 37 \times 109$, we have $N - 1 = 2^6 63$ and $2^{63} \equiv 3521$, $2^{2.63} \equiv -1 \bmod N$. There are no absolute pseudoprimes for the strong test: we shall prove this later.

For numbers $N \equiv 3 \bmod 4$ there are only two terms in the sequence, $b^{\frac{N-1}{2}}$ and b^{N-1} and so the strong test is equivalent to the Euler test. For $N \equiv 1 \bmod 4$ the

strong test is strictly stronger than the Euler test: for example $N = 1105 = 5 \times 13 \times 17$ satisfies $2^{552} \equiv 1 \bmod N$ and so N passes the Euler test, but $2^{276} \equiv 781 \not\equiv \pm 1 \bmod N$ and so N fails the strong test.

Let $N = \prod p_i^{a_i}$, and put $p_i - 1 = 2^{r_i} s_i$. We let $o_2(b \bmod m)$ denote the power of 2 dividing the order of b in the multiplicative group modulo m. The requirement of the strong test base b is that N should pass the Fermat test base b together with the requirement that the value of $o_2\left(b \bmod p_i^{a_i}\right)$ should be the same for every prime power $p_i^{a_i}$ dividing N. If so, we call this common value the *level* of b.

The bases of level 0 are those for which b^s is already $\equiv +1$; the bases of level l are those for which $b^{2^{l-1}s} \equiv -1$ and $b^{2^l s} \equiv +1 \bmod N$.

The multiplicative group modulo p^a projects down onto the multiplicative group modulo p under reduction modulo p: the orders of these groups are $p^{a-1}(p-1)$ and $p-1$ respectively, so the multiplicative order of $b \bmod p^a$ and of $b \bmod p$ differ only by a power of p. For odd p, then, $o_2\left(b \bmod p^a\right) = o_2(b \bmod p)$, and the requirement of the test becomes that the $o_2(b \bmod p)$ should all be equal for p dividing N.

Proposition

If N passes the strong test base b then N also passes the Euler–Jacobi test base b.

Proof: Suppose that $N = \prod p_i^{a_i}$ passes the strong test base b. We must have

$$b^{\frac{N-1}{2}} \equiv \pm 1 \bmod N$$

and we need to show that this sign is the same as $\left(\frac{b}{N}\right)$.

Let l be the level of b, the common value of $o_2(b \bmod p_i)$. For each i, we have $2^l \mid p_i - 1$; put $p_i \equiv 1 + t_i 2^l \bmod 2^{l+1}$ with $t_i = 0$ or 1. Then b is a quadratic residue modulo p_i iff $t_i = 0$; that is, $\left(\frac{b}{p_i}\right) = (-1)^{t_i}$. Now

$$N \equiv \prod_i \left(1 + t_i 2^l\right)^{a_i} \equiv 1 + \sum_i t_i a_i 2^l \bmod 2^{l+1}.$$

Put $T = \sum_i t_i a_i$. We have

$$\left(\frac{b}{N}\right) = \prod_i \left(\frac{b}{p_i}\right)^{a_i} = \prod_i (-1)^{t_i a_i} = (-1)^T.$$

Now $N \equiv 1 + T 2^l \bmod 2^{l+1}$, so T is odd if $l = r$, and even if $l < r$. Since

$$b^{\frac{N-1}{2}} = b^{s 2^{r-1}},$$

we see that in either case $b^{\frac{N-1}{2}} = \left(\frac{b}{N}\right)$, as required. ∎

We observe that the strong test is strictly stronger than the Euler–Jacobi test by considering $N = 6601 = 7 \times 23 \times 41$. We have $2^{1650} \equiv 4509 \bmod 6601$ and $2^{3300} \equiv 1 \bmod 6601$ so that N fails the strong test, but passes the Euler–Jacobi test since $\left(\frac{2}{6601}\right) = +1$.

We can give some indication of the strength of these tests by considering the number of Fermat, Euler–Jacobi and strong pseudoprimes base 2 up to X for X up to 10^{13}.

X	Fermat	Euler–Jacobi	strong
10^4	22	12	5
10^5	78	36	16
10^6	245	114	46
10^7	750	375	162
10^8	2057	1071	488
10^9	5597	2939	1282
10^{10}	14884	7706	3291
25.10^9	21853	11347	4842
10^{11}	38975	20417	8607
10^{12}	101629	53332	22407
10^{13}	264239	139597	58897

Proposition

There are infinitely many strong pseudoprimes base 2.

Proof: Suppose that m is a Fermat pseudoprime base 2: that is, $2^{m-1} \equiv 1 \bmod m$ but m has a non-trivial factor c. Put $N = 2^m - 1$. Since $c \mid m$, we have $2^c - 1 \mid N$, so N is composite. We claim that N is a strong pseudoprime. We have $N - 1 = 2s$ where $s = 2^{m-1} - 1$ is odd. But $s \equiv 0 \bmod m$, so $2^s \bmod N$ is a power of $2^m \bmod N$, and this is just 1 mod N. So $2^s \equiv 1 \bmod N$ and N passes the strong test base 2.

Since N is a Fermat pseudoprime base 2, we can repeat the process and obtain an infinite sequence of strong pseudoprimes base 2. ■

This is far from giving the correct distribution of pseudoprimes.

For numbers in the range $N \leq 10^{12}$, there are 22407 numbers which are strong pseudoprimes base 2; 967 which are strong pseudoprimes bases 2 and 3; 101 are pseudoprimes bases 2,3 and 5; 9 are pseudoprimes bases 2,3,5 and 7; finally, none are pseudoprimes bases 2,3,5,7 and 11. So five rounds of the strong test suffice to completely determine the character of a number of at most 12 decimal digits. A slight improvement in practice might be to perform the strong test bases 2,3,7 and 10 and check for the seven exceptions given below.

For numbers in the range $N \leq 10^{13}$, the strong test with bases 2,3,5,7 and 11 leaves just two exceptions, $2152302898747 = 6763 \times 10627 \times 29947$ and $3474749660383 = 1303 \times 16927 \times 157543$. The latter is a strong pseudoprime for all bases up to and including 16.

N	factors
3215031751	$151 \times 751 \times 28351$
118670087467	172243×688969
128282461501	292441×438661
354864744877	297853×1191409
546348519181	522661×1045321
602248359169	347059×1735291
669094855201	578401×1156801

We need now to consider the probability that a given composite number will pass the strong test to a random base. Unfortunately the set of bases for which N passes the test does not form a subgroup of the multiplicative group modulo N, as had been the case for the previous tests. We can see an example of this for $N = 29341 = 13 \times 37 \times 51$: N is a strong pseudoprime to the bases 2 and 6 but not to the base 3. However the set of such bases is a subset of the set of bases for which N passes the Euler-Jacobi test.

Proposition

Let N have d distinct prime factors. The proportion of bases for which Npasses the strong test is at most 2^{1-d} times the proportion of bases for which N passes the Fermat test.

Proof: The bases for which N passes the strong test form a subset of those for which N passes the Fermat test.

Let $N = \prod_{i=1}^{d} p_i^{a_i}$; put $N - 1 = 2^r s$ and $p_i - 1 = 2^{r_i} s_i$ with s and the s_i odd. For $l \geq 0$, let $c_i(l)$ denote the proportion of $b \bmod p_i^{a_i}$ for which $o_2(b \bmod p_i) = l$.

We have $c_i(0) = 2^{-r_i}$; $c_i(l) = 2^{l-r_i-1}$ for $1 \leq l \leq r_i$ and $c_i(l) = 0$ for $l > r_i$.

The proportion of bases for which N passes the strong test is

$$P = W(N) \sum_{l=0}^{r} \prod_{i=1}^{d} c_i(l).$$

Call this sum S. Put $R = \sum_i r_i$ and let $\rho = \min\{r, r_i\}$. The term $\prod_{i=1}^{d} c_i(l)$ is 2^{-R} for $l = 0$; 2^{dl-R-d} for $l \leq \rho$ and zero otherwise. So

$$S = 2^{-R}\left(1 + \sum_{l=1}^{\rho} 2^{d(l-1)}\right) = 2^{-R}\left(1 + \frac{2^{d\rho} - 1}{2^d - 1}\right)$$

We observe that $R \geq \rho d \geq d \geq 1$.

We have $2^R + 2^1 \geq 2^{R-a} + 2^{1+a}$ for any a with $0 \leq a \leq R - 1$. So

$$2^R + 2 \geq 2^{R+1-d} + 2^d,$$

$$2^{R+1} + 2 \geq 2^R + 2^{R+1-d} + 2^d,$$

$$2^{\rho d} - 1 \leq 2^R - 1 \leq 2^{R+1} - 2^d - 2^{R+1-d} + 1 = \left(2^d - 1\right)\left(2^{R+1-d} - 1\right)$$

$$\frac{2^{\rho d} - 1}{2^d - 1} + 1 \leq 2^{R+1-d}$$

giving $S \leq 2^{1-d}$ as required. ∎

Corollary

If N is composite and $N > 9$, the proportion of bases for which N passes the strong test is at most $\frac{1}{4}$.

Proof: Let d be the number of distinct prime divisors of N. Let P, S be as in the proof above.

If $d = 1$ then N is a prime power, say $N = p^a$. The multiplicative group modulo N is cyclic and $\text{hcf}(N-1, \phi(N-1)) = p - 1$. So $W(N) = \dfrac{p-1}{N-1} \leq \dfrac{1}{p+a} \leq \frac{1}{4}$.

If $d = 2$, then N cannot be a Carmichael number, and so $W(N) \leq \frac{1}{2}$ and $S \leq \frac{1}{2}$. If $d \geq 3$ then $S \leq 2^{1-d} \leq \frac{1}{4}$. In either case $P \leq \frac{1}{4}$. ■

This result is best possible: for the Carmichael number $N = 8911 = 7 \times 19 \times 67$, N is a strong pseudoprime to 1728 of the 7128 bases prime to N.

We observed that if N is composite, then N will fail the Euler–Jacobi test for a base b chosen to be a quadratic non-residue of one prime factor of N and a quadratic residue of the others.

We shall prove the next result at the end of the course.

Theorem

Suppose the Extended Riemann Hypothesis holds. Let G be a proper subgroup of the multiplicative group modulo N. There is a positive integer $b \leq 2(\log N)^2$ such that $b \bmod N \notin G$. ■

Corollary

If the Extended Riemann Hypothesis holds, then an integer N is prime if the Euler–Jacobi test returns `probably prime` *for every base $b \leq 2(\log N)^2$.* ■

Corollary

If the Extended Riemann Hypothesis holds, then the questions "Is N prime?" and "Is N composite?" can be answered in polynomial time. ■

Probabilistic tests on ranges

We showed that for a given composite number, the probability of the strong test incorrectly returning `probably prime` on a random base was at most $\frac{1}{4}$.

Much more important in practice is the probability that a number which has passed the strong test is in fact composite. We consider, for example, a process which chooses odd numbers N of a given size uniformly at random and outputs N if it passes r rounds of the strong test with random bases.

Let $\mathcal{M}_k$ denote the sample space of all odd numbers of exactly k bits; let $\mathcal{A}(N)$ be the event that N is chosen; let $\mathcal{Y}_t$ denote the event that a number passes t rounds of the strong test with random bases; let $\mathcal{C}$ denote the event that a number is composite and $\mathcal{P}$ that a number is prime.

We are interested in the probability

$$w(t,k) = \mathbb{P}(\mathcal{C} \mid \mathcal{Y}_t)$$

that a number which has passed t rounds of the strong test is in fact composite.

The result proved in the previous section can be stated in this notation as

$$\mathbb{P}(\mathcal{Y}_1 \mid \mathcal{C}) \leq \tfrac{1}{4}.$$

We shall need a technical lemma on the distribution of primes.

Lemma

(i) If $p(n)$ denotes the n-th prime, then $p(n) \geq n \log n$;

(ii) $\dfrac{1.105\,X}{\log X} \geq \pi(X) \geq \dfrac{X}{\log X}$ *for $X \geq 10^6$;*

(iii) $\mathbb{P}(\mathcal{P}) \geq \dfrac{2.5}{k}$ *for $k \geq 50$.* ■

Our strategy is to find "small" subsets $\mathcal{E}_m$ of $\mathcal{M}_k$ such that if N is composite and not in $\mathcal{E}_m$ then $\mu(N)$, the probability that N passes the strong test, is also small, at most 2^{-m}.

Proposition

For all $k \geq 50$ and $2 \leq m \leq \sqrt{k/2}$ there exists a set $\mathcal{E}_m$ of composite numbers such that

(i) for composite $N \in \mathcal{M}_k \setminus \mathcal{E}_m$, we have $\mu(N) \leq 2^{-m}$;

(ii) $|\mathcal{E}_m|/|\mathcal{M}_k| \leq \dfrac{1.9\,m}{k}\, 2^{2m-k/m}$.

(iii) $|\mathcal{E}_m|/|\mathcal{M}_k| \leq 1.02\; 2^{2m-k/m}$.

Proof: Put $X = 2^k$. We have $|\mathcal{M}_k| = \frac{1}{4}X$. Fix m with $2 \leq m \leq \sqrt{k/2}$ and put $A = 2^{m-1}$, $\delta = 1/m$. Put $Y = \frac{1}{2}X^{\delta}$. Since $k \geq 50$, $\delta k \geq \sqrt{2k} \geq 10$, and $Y \geq \frac{1}{2}2^{10} = 512$.

Suppose $N \in \mathcal{M}_k$, and put $N = \prod_i^d p_i^{a_i}$. For $p_i \mid N$, let $c_i = \mathrm{hcf}(p_i - 1, N - 1)$ and let $b_i = \dfrac{p_i - 1}{c_i}$. We have

$$W(N) = \frac{1}{\phi(N)} \prod_i c_i = \frac{1}{N} \prod_i \frac{1}{b_i}$$

Put

$$\mathcal{E}_m = \{N \in \mathcal{M}_k \mid N \text{ is composite}, b_i < A \text{ for some } p_i \mid N \text{ with } p_i > Y\}.$$

We first need to show (i). Suppose that N is composite and not in $\mathcal{E}_m$.

If $d > m$ then $\mu(N) \leq 2^{-m}W(N) \leq 2^{-m}$, as required. So we suppose that $N \notin \mathcal{E}_m$ and that $d \leq m$.

Suppose first that the prime factors p_i of N satisfy $p_i < Y$. Put $D = \prod_i p_i$. Now N/D is coprime to $N-1$ but divides $\phi(N)$: indeed

$$\phi(N) = N \prod_{p|N} \left(\frac{p-1}{p}\right) = \frac{N}{D} \prod_{p|N} (p-1).$$

Now $D < Y^m$ and $N > \frac{1}{2}X$, so

$$N/D \geq NY^{-m} = N\left(\tfrac{1}{2}X^{\delta}\right)^{-m} \geq \tfrac{1}{2}X/2^{-m}X = 2^{m-1}.$$

Now $W(N) \leq D/N$, so $W(N) \leq 2^{1-m}$ and again $\mu(N) \leq 2^{-m}$.

Finally suppose that N has a prime factor p_i with $b_i > A$. Then $W(N) < 1/A$ and since $\mu(N) \leq W(N)/2$, we have $\mu(N) < 1/2A = 2^{-m}$.

We now prove parts (ii) and (iii). Fix a prime $p > Y$. Suppose $N \in \mathcal{E}_m$ because $p \mid N$ with $p > Y$ and $b < A$. Now $N \equiv 0 \bmod p$ and $N \equiv 1 \bmod c$. Since p and c are coprime, we have $N \equiv p \bmod pc$. The number of such N in $\mathcal{M}_k$ is at most $\frac{1}{2}X/pc$, which is $\frac{1}{2}Xb/p(p-1)$.

Summing over all $p > Y$ and $b < A$, we have

$$|\mathcal{E}_m| \leq \sum_{p>Y} \sum_{b<A} \frac{\frac{1}{2}Xb}{p(p-1)} < \tfrac{1}{4}A^2X \sum_{p>Y} \frac{1}{p(p-1)}.$$

We have

$$\sum_{p>Y} \frac{1}{p(p-1)} < \sum_{\text{odd } n>Y} \frac{1}{n(n-1)}.$$

Now

$$\sum_{n>Y} \frac{1}{n(n-1)} = \sum_{n>Y} \frac{1}{n-1} - \frac{1}{n}$$

and the contribution of the terms corresponding to odd n is at most

$$\left(\frac{Y+1}{Y-1}\right)^2 \frac{1}{2} \frac{1}{Y-1} \leq \frac{0.505}{Y}$$

using the fact that for $k \geq 50$, $Y \geq 512$.

So

$$\frac{|\mathcal{E}_m|}{|\mathcal{M}_k|} \leq \tfrac{1}{4}A^2X \cdot \frac{512}{511} \cdot \frac{1.01}{X^{\delta}} \cdot \frac{4}{X} < 1.02 \cdot 2^{2m-k/m},$$

giving part (iii).

We now prove part (ii). We have

$$\sum_{p>Y} \frac{1}{p(p-1)} \leq \frac{512}{511} \sum_{p>Y} \frac{1}{p^2}.$$

Let $p(n)$ denote the n-th prime number. We have $p(n) > n \log n$ and $\pi(Y) \geq \frac{Y}{\log Y}$ for $Y \geq 2$, so $p(n) > Y$ implies that $n > \frac{Y}{\log(Y)}$: call this bound $g(X)$. Hence

$$|\mathcal{E}_m| \leq \tfrac{1}{4} A^2 X \frac{512}{511} \sum_{n>g(X)} \frac{1}{n^2 (\log n)^2}.$$

Since $\frac{1}{n^2(\log n)^2}$ is decreasing, we can overestimate the sum by an integral:

$$\sum_{n>g(X)} \frac{1}{n^2(\log n)^2} \leq 1.01 \int_{g(X)}^{\infty} \frac{\mathrm{d}t}{t^2(\log t)^2} = \frac{1.01}{g(X)(\log g(X))^2}$$

since $g(t)$ decreases by a factor of at most 1.01 over an interval of length 1 with $t > 2^{50}$. Now

$$g(X) = \frac{Y}{\log(Y)} = \frac{\frac{1}{2}X^{\delta}}{\log(\frac{1}{2}X^{\delta})} > \frac{1}{2\log 2} \frac{X^{\delta}}{\delta k}$$

and

$$\log g(X) > \delta \log X - \log(\delta k) - \log(2 \log 2) > \delta k \log 2 - \log(\delta k) - \log(2 \log 2).$$

We have $\delta k \geq \sqrt{2k} \geq 10$, so $\log g(X) > 0.43 \delta k$. Hence

$$\frac{1.01}{g(X)(\log g(X))^2} < \frac{2.02 \log 2}{\delta k X^{\delta}} \left(\frac{1}{0.43 \delta k} \right)^2 < \frac{7.58}{\delta k X^{\delta}}$$

whence

$$|\mathcal{E}_m| \leq 1.9 \frac{A^2 m}{k} X^{1-\delta}.$$

Finally, we put $A = 2^{m-1}$ and $|\mathcal{M}_k| = X/4$ and part (ii) follows. ■

These estimates are not necessarily good approximations. For example, for $k = 51$, $m = 3$ the proposition gives an estimate $|\mathcal{E}_3| \leq 2^{34.84}$. This set is the set of Carmichael numbers with just three prime factors between 2^{50} and 2^{51} and direct computation shows that there are just $32035 < 2^{15}$ of these.

Proposition

For $3 \leq v \leq \sqrt{k/2}$ we have

$$w(t,k) \leq \frac{1}{\mathbb{P}(\mathcal{P})} \left(\sum_{m=3}^{v} \mathbb{P}(\mathcal{E}_m) 2^{-t(m-1)} + 2^{-tv} \right)$$

and

$$w(t,k) \leq \sum_{m=3}^{v} \frac{\mathbb{P}(\mathcal{E}_m)}{\mathbb{P}(\mathcal{P})} 2^{-t(m-1)} + 2^{-v(t-1)} \frac{w(1,k)}{1-w(1,k)}.$$

Proof: We have $\mathcal{E}_{m-1} \subseteq \mathcal{E}_m$.

$$\begin{aligned}\mathbb{P}(\mathcal{C} \mid \mathcal{Y}_t) &= \mathbb{P}(\mathcal{E}_3 \mid \mathcal{Y}_t) + \sum_{m=4}^{v} \mathbb{P}((\mathcal{E}_m \setminus \mathcal{E}_{m-1}) \mid \mathcal{Y}_t) + \mathbb{P}((\mathcal{C} \setminus \mathcal{E}_v) \mid \mathcal{Y}_t) \\ &= \frac{\mathbb{P}(\mathcal{E}_3 \cap \mathcal{Y}_t)}{\mathbb{P}(\mathcal{Y}_t)} + \sum_{m=4}^{v} \frac{\mathbb{P}((\mathcal{E}_m \setminus \mathcal{E}_{m-1}) \cap \mathcal{Y}_t)}{\mathbb{P}(\mathcal{Y}_t)} + \frac{\mathbb{P}(\neg\mathcal{E}_v \cap \mathcal{C} \cap \mathcal{Y}_t)}{\mathbb{P}(\mathcal{Y}_t)}\end{aligned}$$

For the first term we use $\mathbb{P}(\mathcal{Y}_1 \mid \mathcal{C}) \leq \frac{1}{4}$ to obtain

$$\mathbb{P}(\mathcal{E}_3 \cap \mathcal{Y}_t) = \mathbb{P}(\mathcal{Y}_t \mid \mathcal{E}_3)\mathbb{P}(\mathcal{E}_3) \leq 2^{-2t}\mathbb{P}(\mathcal{E}_3)$$

For $m \geq 4$ we use part (i) of the previous result to obtain

$$\mathbb{P}((\mathcal{E}_m \setminus \mathcal{E}_{m-1}) \cap \mathcal{Y}_t) = \mathbb{P}(\mathcal{Y}_t \mid \mathcal{E}_m \setminus \mathcal{E}_{m-1})\mathbb{P}(\mathcal{E}_m \setminus \mathcal{E}_{m-1}) \leq 2^{t(1-m)}\mathbb{P}(\mathcal{E}_m)$$

and for the final term we have

$$\mathbb{P}(\neg\mathcal{E}_v \cap \mathcal{C} \cap \mathcal{Y}_t) = \mathbb{P}(\mathcal{Y}_t \mid \mathcal{C} \setminus \mathcal{E}_v)\mathbb{P}(\mathcal{C} \setminus \mathcal{E}_v) \leq 2^{-tv}\mathbb{P}(\mathcal{C}) \leq 2^{-tv}.$$

We have $\mathcal{P} \subseteq \mathcal{Y}_t$, so $\dfrac{1}{\mathbb{P}(\mathcal{Y}_t)} \leq \dfrac{1}{\mathbb{P}(\mathcal{P})}$. Substituting, we have the first result.

We can also write

$$\mathbb{P}(\mathcal{C} \mid \mathcal{Y}_t) \leq \sum_{m=3}^{v} \frac{\mathbb{P}(\mathcal{E}_m)}{\mathbb{P}(\mathcal{Y}_t)} 2^{-t(m-1)} + \frac{\mathbb{P}(\mathcal{Y}_t \mid \mathcal{C} \setminus \mathcal{E}_v)\mathbb{P}(\mathcal{C} \setminus \mathcal{E}_v)}{\mathbb{P}(\mathcal{Y}_t)}$$

so

$$\mathbb{P}(\mathcal{Y}_t \mid \mathcal{C} \setminus \mathcal{E}_v) \leq \mathbb{P}(\mathcal{Y}_1 \mid \mathcal{C} \setminus \mathcal{E}_v)2^{-v(t-1)}$$

and

$$\mathbb{P}(\mathcal{Y}_1 \mid \mathcal{C} \setminus \mathcal{E}_v) = \frac{\mathbb{P}(\mathcal{Y}_1 \cap \mathcal{C} \cap \neg\mathcal{E}_v)}{\mathbb{P}(\mathcal{C} \setminus \mathcal{E}_v)} \leq \frac{\mathbb{P}(\mathcal{Y}_1 \cap \mathcal{C})}{\mathbb{P}(\mathcal{C} \setminus \mathcal{E}_v)} = \frac{\mathbb{P}(\mathcal{Y}_1 \mid \mathcal{C})\mathbb{P}(\mathcal{C})}{\mathbb{P}(\mathcal{C} \setminus \mathcal{E}_v)}.$$

So the final term in the upper bound for $\mathbb{P}(\mathcal{C} \mid \mathcal{Y}_t)$ is at most

$$\frac{\mathbb{P}(\mathcal{Y}_t \mid \mathcal{C} \setminus \mathcal{E}_v)\mathbb{P}(\mathcal{C} \setminus \mathcal{E}_v)}{\mathbb{P}(\mathcal{Y}_t)} \leq 2^{-v(t-1)} \frac{\mathbb{P}(\mathcal{Y}_1 \mid \mathcal{C})\mathbb{P}(\mathcal{C})}{\mathbb{P}(\mathcal{Y}_t)} = 2^{-v(t-1)} \frac{\mathbb{P}(\mathcal{C} \mid \mathcal{Y}_1)\mathbb{P}(\mathcal{Y}_1)}{\mathbb{P}(\mathcal{Y}_t)}.$$

We now have

$$\mathbb{P}(\mathcal{C} \mid \mathcal{Y}_t) \leq \sum_{m=3}^{v} \frac{\mathbb{P}(\mathcal{E}_m)}{\mathbb{P}(\mathcal{P})} 2^{-t(m-1)} + 2^{-v(t-1)} \frac{\mathbb{P}(\mathcal{C} \mid \mathcal{Y}_1)\mathbb{P}(\mathcal{Y}_1)}{\mathbb{P}(\mathcal{Y}_t)}.$$

Finally,

$$\mathcal{Y}_y \supseteq \mathcal{P} = \mathcal{P} \cap \mathcal{Y}_1 = \mathcal{Y}_1 \setminus (\mathcal{C} \cap \mathcal{Y}_1),$$

so

$$\mathbb{P}(\mathcal{Y}_t) \geq \mathbb{P}(\mathcal{Y}_1) - \mathbb{P}(\mathcal{C} \cap \mathcal{Y}_1) = \mathbb{P}(\mathcal{Y}_1) - \mathbb{P}(\mathcal{C} \mid \mathcal{Y}_1)\mathbb{P}(\mathcal{Y}_1)$$

giving

$$\frac{\mathbb{P}(\mathcal{Y}_1)}{\mathbb{P}(\mathcal{Y}_t)} \leq \frac{1}{1-\mathbb{P}(\mathcal{C}|\mathcal{Y}_1)}$$

and the result follows. ■

Theorem

For $k \geq 50$, we have
for $1 \leq t \leq 4$,

$$w(t,k) \leq 0.4\,k\left(1+2^t\right)\left(2^{t-t\sqrt{k/2}}\right);$$

for $5 \leq t \leq k/9+2$,

$$w(t,k) \leq 0.4\,k2^t\left(2^{-2\sqrt{k(t-2)}}+2^{-t\sqrt{k/2}}\right);$$

and for $t > k/9+2$,

$$w(t,k) \leq 0.4\,k\left(64\cdot 2^{-2t-k/3}+2^{t-t\sqrt{k/2}}\right).$$

Proof: Let M be the integer part of $\sqrt{k/2}$. Using the first part of the previous proposition with $v = M$, we have

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

The definition of M implies that $2^{-tM} \leq 2^{-t\left(\sqrt{k/2}-1\right)}$ and from Lemma 1 (iii) we have

$$\frac{1}{\mathbb{P}\left(\mathcal{P}\right)} \leq 0.4\,k$$

By the previous result,

$$\sum_{m=3}^{M}\mathbb{P}\left(\mathcal{E}_m\right)2^{-t(m-1)} \leq \frac{1.2\,2^t}{\sqrt{2k}}\sum_{m=3}^{M}2^{(2-t)m-k/m}.$$

Put $g(m) = 2^{(2-t)m-k/m}$ and $S = \sum_{m=3}^{M} g(m)$.

For $1 \leq t \leq 4$, the function $g(m)$ is increasing between 3 and M and we can estimate the sum S by the final term multiplied by the number of terms:

$$S \leq Mg(M) \leq \sqrt{k/2}\,2^{-t\sqrt{k/2}}.$$

For $5 \leq t \leq \dfrac{k}{9}+2$ the maximum value of $g(m)$ is attained at $m_0 = \sqrt{k/(t-2)}$ and this lies between 3 and M. We have

$$S \leq Mg(m_0) \leq \sqrt{k/2}\,2^{-2\sqrt{k(t-2)}}.$$

For $t > \dfrac{k}{9}+2$, the function $g(m)$ decreases from $m = 3$ and

$$S \leq Mg(3) \leq \sqrt{k/2}\,2^{-(t-2)3-k/3}.$$

■

Let us consider the case $k = 250$ (about 75 decimal digits). For $t = 6$, the Theorem gives

$$w(6, 250) \leq 0.4 \cdot 6 \cdot 2^6 \left(2^{-2\sqrt{250.4}} + 2^{-6\sqrt{125}}\right) < 2^{-56}.$$

Theorem

For $k \geq 50$, we have
for $1 \leq t \leq 4$,

$$w(t, k) \leq 0.4\, k\, 2^t \left(1 + 0.721\sqrt{k}\right) \left(2^{-t\sqrt{k/2}}\right);$$

for $5 \leq t \leq k/9 + 2$,

$$w(t, k) \leq 0.4\, k\, 2^t \left(0.721\sqrt{k}\, 2^{-2\sqrt{k(t-2)}} + 2^{-t\sqrt{k/2}}\right);$$

and for $t > k/9 + 2$,

$$w(t, k) \leq 0.4\, k \left(46.2\sqrt{k}\, 2^{-2t-k/3} + 2^{t-t\sqrt{k/2}}\right).$$

Proof: Let M be the integer part of $\sqrt{k/2}$. Using the first part of the previous proposition with $v = M$, we have

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

The definition of M implies that $2^{-tM} \leq 2^{-t\left(\sqrt{k/2}-1\right)}$ and we have

$$\frac{1}{\mathbb{P}(\mathcal{P})} \leq 0.4\, k.$$

We have

$$\sum_{m=3}^{M} \mathbb{P}(\mathcal{E}_m) 2^{-t(m-1)} \leq \frac{1.02\sqrt{k}\, 2^t}{\sqrt{2k}} \sum_{m=3}^{M} 2^{(2-t)m - k/m}$$

by the previous result. Define $g(m) = 2^{(2-t)m-k/m}$ and $S = \sum_{m=3}^{M} g(m)$.

For $1 \leq t \leq 4$, the function $g(m)$ is increasing between 3 and M and we can estimate the sum S by the final term multiplied by the number of terms:

$$S \leq M g(M) \leq \sqrt{k/2}\, 2^{-t\sqrt{k/2}}$$

which again gives the result stated.

For $5 \leq t \leq \dfrac{k}{9} + 2$, the maximum value of $g(m)$ is attained at $m_0 = \sqrt{k/(t-2)}$ and this lies between 3 and M. We have

$$S \leq M g(m_0) \leq \sqrt{k/2}\, 2^{-2\sqrt{k(t-2)}}.$$

For $t > \frac{k}{9} + 2$, the function $g(m)$ decreases from $m = 3$ and we estimate the sum S by the first term multiplied by the number of terms:

$$S \leq Mg(3) \leq \sqrt{k/2}\, 2^{-(t-2)3-k/3}.$$

■

Let us consider the case $k = 1000$ (about 300 decimal digits) and $t = 10$. We have

$$w(10, 1000) \leq 2^{-165}$$

Primality proofs and tests

In the previous sections we discussed probabilistic tests based on Fermat's little theorem and estimated the probability of an incorrect return.

We now turn to algorithms for proving primality.

Proposition

Suppose that $N-1$ has prime power factorisation $N-1 = \prod_{i=1}^{d} q_i^{e_i}$. If there exists a_i for $i = 1, \ldots, d$ such that

$$a_i^{N-1} \equiv 1 \bmod N$$

and

$$\text{hcf}\left\{a_i^{\frac{N-1}{q_i}} - 1, N\right\} = 1$$

then N is prime.

Proof: Let p be a prime factor of N. The conditions on a_i imply that $a_i^{N-1} \equiv 1 \bmod p$ and $a_i^{(N-1)/q_i} \not\equiv 1 \bmod p$. Hence $b_i = a_i^{(N-1)/q_i^{e_i}}$ is also not $1 \bmod p$. So b_i is an element of order exactly $q_i^{e_i}$ modulo p, and so $p \equiv 1 \bmod q_i^{e_i}$. Since this is true for all i, we have $N - 1 \mid p - 1$, so $N = p$ is prime. ■

Theorem

The question "Is N prime?" can be answered in non-deterministic polynomial time.

Proof: Put $l = \log_2 N$. We claim that there is a certificate of length at most $2l^3$ which can be used to verify the primality of N in time polynomial in l. We may assume $l \geq 4$.

We apply the previous result to a certificate consisting of a list comprising the factors q_i, the corresponding a_i, and the certificates for each of the $q_i > 2$: the claim is that this certificate has length at most $2l^3$. We proceed by induction on N. Put $l_i = \log_2 q_i$.

The number of distinct prime factors $N - 1$ is at most l, so the number of q_i and a_i is at most l and the number of bits in each a_i is at most $l + 1$. By the induction hypothesis, the length of the certificate for each q_i is of length at most $2l_i^3$. Since we may assume N odd, we have $\sum_{i>1} l_i \leq l - 1$. So

$$\sum_{i>1} l_i^3 \leq \left(\sum_{i>1} l_i\right)^3 \leq (l-1)^3 \leq l^3 - 2l^2 - l$$

for $l \geq 4$ and the total length of the certificate for N is at most $2(l^3 - 2l^2 - l) + 2l(l+1) = 2l^3$, as required.

Since the requirements on the a_i can clearly be checked in polynomial time, the result follows. ■

Clearly for general N, the task of factorising $N - 1$ is not likely to be practical, but the theorem is of value for numbers of special form.

We give a proof that $n = 27! + 1 = 10888869450418352160768000001$ is prime. The prime factorisation of

$$n - 1 = \prod_i q_i^{e_i} = 2^{23} \cdot 3^{13} \cdot 5^6 \cdot 7^3 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23$$

and we take $a = 37$ (found by experiment).

q	t	$\mathrm{hcf}\{t-1, n\}$	$t^q \bmod n$
2	108888694504183521607680000000	1	1
3	935401096397349291699351241 4	1	1
5	135101251602649907065383076 2	1	1
7	806281304530494479736977103 9	1	1
11	246373320901407720727827 8496857	1	1
13	640726896179474170271027 3269	1	1
17	905336135231200195795145 5964	1	1
19	835692648514178922966049 4702	1	1
23	382778117363357064316660 5750	1	1

In the previous example, $p - 1$ was easy to factor (indeed of special form). Consider now the case of $P = 2 \cdot 10^{63} + 2 \cdot 10^{36} + 2 \cdot 10^{12} + 2293$. We check that P is a probable prime by the Miller–Rabin test. Factorising, we find that $P - 1 = 2^2 \cdot 3 \cdot 83 \cdot 293 \cdot 4759 \cdot 7396423814267 \cdot Q$ where $Q = 19469981724133230705850011347128038898061 3$ is a probable prime: the factorisation is not trivial. A similar table shows $t = 2^{(P-1)/q} \bmod P$ as q runs over the prime factors of $P - 1$ (experiment showed that taking $a = 2$ was always sufficient).

q	t	$\mathrm{hcf}\{t-1, n\}$	$t^q \bmod n$
2	2000000000000000000000000000020000000000000000000000002000000002292	1	1
3	131815308659173173646992072684362164139392980059854336182627750 6	1	1
83	692025363589515413419308200391678011962581291998221072585535812	1	1
293	158011123791168237563028434747621928540969790134697531180064224 9	1	1
4759	962702317170486488839666372340353723257412185628764648899805234	1	1
7396423814267	163936032731929144668897127339282473907215770606654346214485199 3	1	1
Q	110455157815949727733773088760854738403986398017028160780256102 1	1	1

Proving the primality of p now reduces to proving that of the alleged prime factors of $p - 1$: especially Q. We might accept proving the primality of 7396423814267 bu trial division, but need to to better with Q. Factoring, we find $Q - 1 = 2^2 \cdot 179251335702611 \cdot 271545838805284119171584123$ and that, again taking $a = 2$, we reduce the proof of the primality of Q to that of 179251335702611 and of 271545838805284119171584123.

Taking $p = 271545838805284119171584123$, we have $p - 1 = 2 \cdot 31 \cdot 97 \cdot 223 \cdot 10475971813 \cdot 19327716377$.

We may repeat the process to find proofs of the primality of these numbers also.

We summarise in the table below, assuming that we need no further proof for primes under 10^6.

p	a	p	a	p	a	p	a	p	a	p
P	2	2								
	2	3								
	2	83								
	2	293								
	2	4759								
	2	7396423814267	2	2						
			2	328333						
			2	11263601	2	2				
					2	5				
					2	29				
					2	971				
	2	Q	2	2						
			2	179251335702611						
			2	271545838805284119171584123	2	2				
					2	31				
					2	97				
					2	223				
					2	10475971813	2	2		
							3	3		
							2	17		
							2	5705867	2	2
									2	29
									2	98377
					2	19327716377	3	2		
							2	47		
							2	9		
							2	529933		

Define the n^{th} *Fermat number* by $F_n = 2^{2^n} + 1$. The Fermat numbers, $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ and $F_4 = 65537$ are all prime. The next is composite, $F_5 = 4294967297 = 641 \times 6700417$, and all subsequent Fermat numbers for which the character has been determined are also composite.

The largest known composite Fermat number is F_{23471}. The Fermat numbers up to F_{21} are known to be composite, and those up to F_{13} have been factorised.

Put $N = F_n$, so that $N - 1 = 2^{2^n}$ is fully factorised. If we can find b such that $b^{2^{n-1}} - 1$ is prime to N, then N is prime. Consider the Euler–Jacobi test applied to N base b. For N to pass the test, we must have $b^{2^{n-1}} \equiv \left(\frac{b}{N}\right)$ and if $b^{2^{n-1}} - 1$ is prime to N this means that $\left(\frac{b}{N}\right)$ must be -1 rather than $+1$.

We see therefore that N is prime iff for b such $\left(\frac{b}{N}\right) = -1$ we have $b^{2^{n-1}} \equiv -1$. For $n \geq 1$, $F_n \equiv 2 \bmod 3$ and $\equiv 1 \bmod 4$, so $\left(\frac{3}{N}\right) = \left(\frac{N}{3}\right) = -1$.

We have proved

Proposition

The Fermat number F_n, for $n \geq 1$, is prime if and only if $3^{2^{n-1}} \equiv -1 \bmod N$. ■

We can use the argument of the Theorem to obtain useful information about numbers N for which $N - 1$ is not completely factorised.

Theorem

Suppose that $N - 1 = FC$ where $F = \prod_{i=1}^{d} q_i^{e_i}$ is fully factorised. If there exists a_i for $i = 1, \ldots, d$ such that

$$a_i^{N-1} \equiv 1 \bmod N$$

and

$$\text{hcf}\left\{a_i^{\frac{N-1}{q_i}} - 1, N\right\} = 1$$

then every prime factor p of N satisfies $p \equiv 1 \bmod F$.

Proof: Let p be a prime factor of N. As before, $p \equiv 1 \bmod q_i^{e_i}$ for each i and so $F \mid p - 1$. ■

Corollary

If N satisfies the conditions of the Theorem with $F > C$ then N is prime.

Proof: If N is composite, it has at least one prime factor $p \leq \sqrt{N}$. But by the Theorem, $p > F$ and $N = FC + 1 \leq F^2$, so $p > \sqrt{N}$, a contradiction. ■

The discussion of Fermat numbers generalises immediately to the next result.

Proposition

Suppose that $N-1 = 2^r s$ with $s < 2^r$. If there is a base b mod N for which N passes the Euler test in the form $b^{\frac{N-1}{2}} \equiv -1 \bmod N$, then N is prime. ■

Clearly one should look for bases with $\left(\frac{b}{N}\right) = -1$.

We can use these results to construct classes of provable primes. Suppose that $\mathcal{L}$ is a list of proved primes: for example we might begin by taking $\mathcal{L}$ to be the set of all primes up to some limit L. We let F be a random product of elements of $\mathcal{L}$, take C a random number less than F and put $N = FC + 1$. We now test N for primality by some fast probabilistic test, such as the Miller–Rabin test. If N passes this test, it is worth attempting to to prove the primality of N using the results above. If N is proved prime then N can be added to $\mathcal{L}$ and the procedure repeated.

Quadratic tests

All the tests we have considered up to now rely on properties of the ring of integers modulo N, which will be a field precisely when N is prime. The tests depend to a considerable extent on properties of the multiplicative group and examination of various subgroups and in particular on the factorisation of its putative order $N-1$. For example, the strength of the Miller–Rabin test is greatest when $N-1$ is divisible by a high power of 2, and the primality proofs just discussed rely on being able to obtain at least a partial factorisation of $N-1$.

Let us now consider what to do if $N-1$ has an inconvenient factorisation: for example, suppose $N-1 = 2pq$ where p and q are large primes.

We construct a new series of tests by working in the quadratic ring $\mathbb{Z}/N[\sqrt{d}]$. For any ring R, we define $R[\sqrt{d}]$ to be the ring of elements of the form $x + y\sqrt{d}$, with $x, y \in R$ and addition and multiplication given by the rules

$$\left(u + v\sqrt{d}\right) + \left(x + y\sqrt{d}\right) = u + x + (v + y)\sqrt{d}$$

and

$$\left(u + v\sqrt{d}\right)\left(x + y\sqrt{d}\right) = ux + dvy + (uy + vx)\sqrt{d}.$$

Inversion in the ring modulo N is achieved by

$$\left(x + y\sqrt{d}\right)^{-1} = \frac{x - y\sqrt{d}}{x^2 + dy^2}$$

provided that the *norm* $x^2 + dy^2$ is invertible in R.

The ring $\mathbb{Z}/N[\sqrt{d}]$ can be obtained as the quotient of the polynomial ring $\mathbb{Z}[X]$ by the ideal $\langle X^2 - d, N\rangle$.

For prime p the ring $\mathbb{Z}/p[\sqrt{d}]$ is a field iff the polynomial $X^2 - d$ is irreducible in $\mathbb{Z}/p$: that is, iff d is a quadratic non-residue of p. In this case, the ring $\mathbb{Z}/p[\sqrt{d}]$ is the finite field GF (p^2) of order p^2.

If d is a quadratic residue modulo p, say $d \equiv e^2 \bmod p$, then the ring $\mathbb{Z}/p[\sqrt{d}]$ is isomorhpic to a direct sum of two copies of $\mathbb{Z}/p$,

$$\mathbb{Z}/p[\sqrt{d}] \xrightarrow{\sim} \mathbb{Z}/p \oplus \mathbb{Z}/p$$

by

$$x + y\sqrt{d} \mapsto (x + ye, x - ye).$$

We can generalise the construction by considering a quadratic polynomial $f(X) = X^2 + bX + c$ with discriminant $d = b^2 - 4c$. The quotient ring $\mathbb{Z}/\langle N, f(X)\rangle$ will then be $\mathbb{Z}/N[\sqrt{d}]$.

When $\mathbb{Z}/p[\sqrt{d}]$ is a field GF (p^2), the multiplicative group is cyclic of order p^2-1. We define the *rational* subgroup to be the elements $x + y\sqrt{d}$ with $y = 0$, that is, the elements of the multiplicative group modulo p. Further define the *co-rational* subgroup to be the quotient group $\mathbb{Z}/p[\sqrt{d}]^*/\mathbb{Z}/p^*$, consisting of classes of rational multiples of $x + y\sqrt{d}$. The co-rational group has order $p + 1$.

We can now form an analogue of the Fermat test for the co-rational group. The *Lucas test* for N proceeds as follows. Given N, pick any auxiliary d such that $d \not\equiv 0 \bmod N$. If $\mathrm{hcf}(d, N) > 1$ then N is `composite`. Otherwise pick a base $\beta = x + y\sqrt{d} \bmod N$. If $\mathrm{hcf}(\beta\bar{\beta}, N) > 1$ then again N is `composite`. The test now requires that $\beta^N \equiv x + \left(\frac{d}{N}\right) y\sqrt{d} \bmod N$: if this holds, return `probably prime`, otherwise `composite`.

Proposition

If N is prime, then N passes the Lucas test.

Proof: Suppose N is prime. Choose d prime to N and let $\beta = x + y\sqrt{d}$.

If $\left(\frac{d}{N}\right) = +1$ then the ring $\mathbb{Z}/N[\sqrt{d}]$ is isomorphic to two copies of $\mathbb{Z}/N$, so the multiplicative group $\mathbb{Z}/N[\sqrt{d}]^*$ has exponent $N - 1$ and we have $\beta^N = \beta$. If $\left(\frac{d}{N}\right) = -1$ then $\mathbb{Z}/N[\sqrt{d}]$ is a field and the Frobenius map $\xi \mapsto \xi^N$ is the unique non-trivial automorphism, which must be conjugation. So $\beta^N = x - y\sqrt{d}$. ∎

When $\left(\frac{d}{N}\right) = -1$, the Lucas test can be regarded as the analogue of the Fermat test for the rational and co-rational group simultaneously. Suppose N passes the test base β. Put $b = \beta\bar{\beta}$. If $\beta^N = \bar{\beta}$ then $\bar{\beta}^N = \bar{\bar{\beta}} = \beta$, so

$$b^{N-1} = \beta^{N-1}\bar{\beta}^{N-1} = \frac{\bar{\beta}}{\beta}\frac{\beta}{\bar{\beta}} = 1,$$

which is the identity in the rational group, and

$$(\beta/\bar{\beta})^{N+1} = \beta\bar{\beta} = b,$$

which is the identity in the corational group.

Just as in the case of the Fermat test, it is possible for a composite number to pass the test. An example with $\left(\frac{d}{N}\right) = +1$ can be constructed easily out of a Fermat pseudoprime. Let $N = 341 = 11 \times 31$, and let $d = 5$. Put $\beta = 3 + 212\sqrt{5} \bmod 341$. Then $\beta^{341} = \beta$. Since $37^2 \equiv 5 \bmod 341$ and $212 \cdot 37 \equiv 1 \bmod 341$ then in the isomorphism

$$\mathbb{Z}/341[\sqrt{5}] \xrightarrow{\sim} \mathbb{Z}/341 \oplus \mathbb{Z}/341$$

defined by $\sqrt{5} \mapsto (37, -37)$ we have $\beta \mapsto (4, 2)$ and 341 is a Fermat pseudoprime to the bases 2 and 4.

In this case, we also have *absolute* psuedoprimes, the analogues of Carmichael numbers. The smallest two known are are $443372888629441 = 17 \times 31 \times 41 \times 43 \times 89 \times 97 \times 167 \times 331$ and $39671149333495681 = 17 \times 37 \times 41 \times 71 \times 79 \times 97 \times 113 \times 131 \times 191$, both of which have the property that for any d with $\left(\frac{d}{N}\right) = +1$, a base β can fail the Lucas test only when the norm of β has a factor in common with N. Such numbers have the property that if $p \mid N$ then $p^2 - 1 \mid N - 1$, and so are Carmichael numbers in particular.

When $\left(\frac{d}{N}\right) = -1$, we can again find pseudoprimes. Consider $N = 2465 = 5 \times 17 \times 29$ and $d = 3$. Put $\beta = -73 + 226\sqrt{3}$. Then $\beta^N \equiv \bar{\beta}\beta = 1$.

In this case, however, there are no absoulte pseudoprimes.

The Lucas test clearly contains the Fermat test: whatever d, if we take β to be rational, then the Lucas test requires that $\beta^N = \beta$, which is the Fermat test. However, if we take $\beta = \sqrt{d}$, then the Lucas test requires that $\beta^N = \left(\frac{d}{N}\right)\beta$. But this is just $\sqrt{d}^{N-1} = \left(\frac{d}{N}\right)$, that is, $d^{\frac{N-1}{2}} = \left(\frac{d}{N}\right)$, which is the Euler–Jacobi test.

The computation of β^N in the Lucas test can be carried out by the usual square and multiply method using the definitions of multiplication in the ring $\mathbb{Z}/N[\sqrt{d}]$ given above. There is another method of formulating the calculation which avoids the use of the quadratic extension.

Let $\beta = x + y\sqrt{d}$ and suppose that $f(X) = X^2 - 2xX + b$ is the quadratic polynomial satisfied by β over $\mathbb{Z}/N$, where $b = x^2 - dy^2$ is the norm of β. Put $\beta^n = x_n + y^n\sqrt{d}$. Then $x_0 = 1$, $y_0 = 0$, $x_1 = x$ and $y_0 = y$. The sequences x_n and y_n both satisfy the recurrence relation $z_{n+1} = 2xz_n - bz_{n-1}$.

The Lucas test can now be phrased as requiring that for any polynomial $f(X) = X^2 - aX + b$, any sequence y_n with $y_0 = 0$ and satisfying the recurrence relation $y_{n+1} = ay_n - by_{n-1}$ has $y_N = \left(\frac{a^2 - 4b}{N}\right)y_1$.

The analogue of the results proved earlier can be summarised in the following result.

Proposition

Suppose that $N + 1 = FC$ where $F = \prod_{i=1}^{d} q_i^{e_i}$ is fully factorised. If there exist d with $\left(\frac{d}{N}\right) = -1$ and elements β_i in $\mathbb{Z}/N[\sqrt{d}]$ of norm 1 for $i = 1, \ldots, d$ such that

$$\beta_i^{N+1} \equiv 1 \bmod N$$

and

$$\text{hcf}\left\{\beta_i^{\frac{N+1}{q_i}} - 1, N\right\} = 1$$

then every prime factor p of N satisfies $p \equiv \left(\frac{d}{p}\right) \bmod F$. In particular, $p \geq F$.

Proof: Let p be a prime factor of N. The conditions on β_i imply that $\beta_i^{N+1} \equiv 1 \bmod p$ and $\beta_i^{(N+1)/q_i} \not\equiv 1 \bmod p$ in the group $\mathbb{Z}/p[\sqrt{d}]$. Hence $\gamma_i = \beta_i^{(N+1)/q_i^{e_i}}$ is also not $1 \bmod p$. So γ_i is an element of order exactly $q_i^{e_i}$ modulo p, and so $q_i^{e_i} \mid p - \left(\frac{d}{p}\right)$. Since this is true for all i, $F \mid p - \left(\frac{d}{p}\right)$. ■

Corollary

If N satisfies the conditions of the proposition and $F > C$ then N is prime. ■

We define the *Mersenne number* $M_p = 2^p - 1$. If p is composite then M_p is composite, so we restrict our attention to p prime.

In order to prove $N = M_p$ prime by the Lucas test, we need to find a d with $\left(\frac{d}{N}\right)$ and a β which is not a square in the co-rational group. We see that $M_p \equiv 1 \bmod 3$ and so $\left(\frac{3}{N}\right) = -1$. The element $\beta = 2 + \sqrt{3}$ of the circle group is easily found by inspection†. We need to consider whether β represents an element of maximal order in the corational group: that is, whether β has a square root in the circle group. Since 2 has order p in the multiplicative group modulo M_p, and the order of this group is even, 2 is a square; let $\sqrt{2}$ denote a square root modulo M_p. By direct calculation, $\beta = \gamma^2$ where $\gamma = \frac{1+\sqrt{3}}{\sqrt{2}}$. The norm of γ is -1. We have $\beta^{\frac{N+1}{2}} = \gamma^{N+1} = \gamma\bar{\gamma} = -1$.

Since $N + 1 = 2^p$ is fully factored, we have proved

Proposition

The Mersenne number M_p is prime if and only if p is prime and

$$\left(2 + \sqrt{3}\right)^{\frac{M_p+1}{2}} \equiv -1 \bmod M_p.$$

■

This test can be programmed to run very fast in practice, using fast modular multiplication techniques, and so the largest known prime at any given time is usually a Mersenne number. At present‡, the largest known prime is $M_{1257787}$. The previous holders of the title were M_{859433} [1994], M_{756839} [1992], $391581 \cdot 2^{216193} - 1$ [1989] and M_{216091} [1985]. The largest known twin primes are $1706595 \cdot 2^{11235} \pm 1$.

† It is the fundamental unit of the ring $\mathbb{Z}[\sqrt{3}]$.

‡ 3rd September 1996

1 Elliptic curves

We cannot do more than give a very brief introduction to elliptic curves in this section. See Cassels [4], [5], Husemöller [14], Knapp [16], Silverman [28], and chapters in Cohen [7] and Niven *et al* [26].

1.1 Elliptic curves over any field

An *elliptic curve* over a field F can be defined as a non-singular projective plane cubic curve. In general, we can write such a curve in *Weiserstrass* form $Y^2 = X^3 + aX + b$, with the cubic in X having distinct roots (that is, non-zero discriminant $\Delta = -4a^3 - 27b^2$). Over fields of characteristic 2 or 3 we need a more general form

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

In addition to the *affine* points, there is a single *point at infinity*, $\mathcal{O} = (0 : 1 : 0)$ in projective coordinates. It is a point of inflexion for E: that is, the tangent has triple contact.

If K is a field containing the field of definition F, we define $E(K)$ to be the set of points (always including $\mathcal{O}$) with coordinates in K.

•The points $E(K)$ form an abelian group with $\mathcal{O}$ as zero. □

The group law is defined by the "tangent–chord" process. We note that a line has at most three points of intersection with E, and exactly three if counted according to multiplicity. We define points P, Q, R to sum to zero iff they are collinear. So if P and Q are in $E(K)$, then the equation of the chord joining them (or if $P = Q$, the equation of the tangent) is defined over K, and hence so is the third solution R. Now every vertical line goes through $\mathcal{O}$, so the sum of P and Q is the other point on the vertical line though R.

It is clear that this process defines a commutative binary operation: associativity is the least easy part (but see below). The operations of addition, duplication and negation are given by explicit rational functions with coefficients which are integer polynomials in the coefficients of the Weierstrass equation.

1.1.1 Explicit formulae for the group law

Suppose that we wish to add $P = (x_1, y_1)$ to $Q = (x_2, y_2)$ on the elliptic curve E with equation $Y^2 = X^3 + aX + b$, to obtain $P + Q = (x_3, y_3)$. If $x_1 = x_2$ but $y_1 \neq y_2$, then $P = -Q$ on E, and $P + Q = \mathcal{O}$. Otherwise, let $\ell : Y = mX + c$ be the line intersecting E in P and Q.

If $P \neq Q$, then ℓ has equation $m = \frac{y_2 - y_1}{x_2 - x_1}$ and $c = \frac{x_2y_1 - x_1y_2}{x_2 - x_1}$; if $P = Q$ then $m = \frac{3x_1^2 + a}{2y_1}$ and $c = \frac{2y_1^2 - 3x_1^3 - ax_1}{2y_1}$.

Substituting $Y = mX + c$ into $Y^2 = X^3 + aX + b$, we have $X^3 - m^2X^2 + \ldots = 0$. So the sum of the roots is $x_1 + x_2 + x_3 = m^2$, and the point $P + Q = (x_3, y_3)$ where $y_3 = -(mx_3 + c)$.

Fast algorithms for performing the group operations on an elliptic curve are described by Koyama and Tsuruoka [18].

1.1.2 Division points

The traditional term for a point of finite order in the group structure is *division point.* For example, the 2-division points are the points $(x, 0)$ where x is a root of the cubic $x^3 + ax + b$, since these are the points with vertical tangent, hence $[2]P = \mathcal{O}$.

The map $[n]$ of multiplication by n on E is a rational function, determined by the *division* polynomials. Originally computed by Weber, the fastest algorithm is due to McKee [22], [23]. Computation shows that there are at most n^2 points of order dividing n: the group $E[n]$ of n-division points is of rank at most 2. In general the rank is exactly 2 over a large enough field, except when n is divisible by the characterstic of the field.

If all n^2 points of order n are defined over K, then so is the *Weil pairing*, a non-singular alternating bilinear map with values in n-th roots of unity (necessarily also in K), $W_n : E[n] \times E[n] \to \mu_n$.

1.1.3 The ring of endomorphisms

An endomorphism of E is a rational map from E to E which respects the group structure (indeed every rational map is an endomorphism composed with a translation). Endomorphisms form a ring under composition. Examples are the multiplications $[n]$ by integers: a less obvious example is $(x, y) \mapsto (-x, \mathrm{i}y)$ on $Y^2 = X^3 + X$.

•The ring of endomorphisms of E are either $\mathbf{Z}$, an imaginary quadratic ring, or (in finite characteristic only) a quaternion order. □

When E has non-trivial endomorphisms, we say that it has *complex multiplication*[1]; the quaternion case is *supersingular*.

1.1.4 Models for an elliptic curve

We define the *j-invariant* of the elliptic curve $Y^2 = X^3 + aX + b$ to be $j = -2^8 3^3/\Delta$ where $\Delta = -4a^3 - 27b^2$ is the discriminant. As its name suggests, it is an isomorphism invariant of the curve, and there is at least one curve for every value of j. If j is not 0 or 1728, take $a = -27j(j - 1728)^3$, $b = 54j(j - 1728)^5$ to give a curve with $\Delta = 2^{12}3^{12}j^2(j - 1728)^9$ and invariant j. If $j = 0$, take $a = 0$, $b = 1$ and if $j = 1728$, take $a = 1$, $b = 0$.

In characteristic 2 or 3 the formulae for j and Δ become somewhat more complicated, but the recipe for constructing a curve with the required value of j remains essentially the same.

We define the *twist* of E by d as the curve with equation $dY^2 = X^2 + aX + b$: equivalently, $Y^2 = X^3 + ad^2X + bd^3$. These curves have the same j-invariant and become isomorphic over the extension of the field of definition by $\sqrt{d}$.

1.2 Elliptic curves over the complex numbers

We can obtain the entire theory of elliptic curves over the complex numbers by starting with doubly periodic functions having a lattice $\Lambda = \mathbf{Z}\langle\omega_1, \omega_2\rangle$ of periods. The Weierstrass $\wp$-function satisfies the differential equation $\wp'^2 = 4\wp^3 - g_2\wp - g_3$, and so the pair $(\wp, \wp')$ parametrises the complex torus $\mathbf{C}/\Lambda$ as an elliptic curve. It is now clear that there must be an Abelian group structure. As a Riemann surface the complex points $E(\mathbf{C})$ form a torus, hence have *genus* 1. (There is an algebraic definition of genus over any field.)

The *ubiquity* theorem guarantees that any complex elliptic curve arises in this way (the invariant j is a holomorphic function of the ratio ω_2/ω_1).

We immediately see that

$$E[n] \equiv \frac{1}{n}\Lambda/\Lambda \equiv \mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/n\mathbf{Z}$$

and that the endomorphisms must come from multiplication by elements of Λ. For example, the curve $Y^2 = X^3 + X$ corresponds to $\Lambda = \mathbf{Z}[\mathrm{i}]$.

The Weil pairing is given, for rational numbers a, b, c, d by

$$W(a\omega_1 + b\omega_2, c\omega_1 + d\omega_2) = \exp(2\pi\mathrm{i}(ad - bc)).$$

We construct complex multiplication curves by taking the period lattices to be ideals in complex quadratic rings $\mathbf{Z}[\sqrt{d}]$. The following result is part of the theory of modular forms.

•The complex multiplication curves corresponding to $\mathbf{Z}[\sqrt{d}]$ are defined over an algebraic number field of degree $h(d)$. □

[1] An obsolete term is *singular*.

1.3 Elliptic curves over a finite field

An elliptic curve E over a finite field $F = \mathrm{GF}(q)$ can have only finitely many points. If we consider the quadratic character of the cubic $X^3 + aX + b$ as being random, then the expected number of points on the curve should be about $q + 1$ (remembering to include the point at infinity). In fact this is not far from the truth. If E has N points, write $N = q + 1 - t$ where t is the *trace of Frobenius*[2]. We have *Hasse's Theorem*[3]

•$|t| \leq 2\sqrt{q}$. □

The range of possible values $q+1-2\sqrt{q} \leq N \leq q+1+2\sqrt{q}$ is the *Hasse range*. Every possible value in the range occurs, indeed Birch [2] shows that for curves over a prime field

•The number of elliptic curves with trace of Frobenius t over $\mathrm{GF}(p)$ is given by the class-number $H(t^2 - 4p)$. □

Hasse's theorem implies that the quadratic polynomial $X^2 - tX + q$ cannot have distinct real roots, and complex roots over a prime field. If we let α and $\bar{\alpha}$ denote the roots, then the number of points on E over $\mathrm{GF}(q)$ is $(\alpha - 1)(\bar{\alpha} - 1)$ and the number of points on E over $\mathrm{GF}(q^n)$ is $(\alpha^n - 1)(\bar{\alpha}^n - 1)$.

The torsion in an elliptic curve over a finite field of characteristic p follows the same pattern as over a field of characteristic zero, with the exception of the p-torsion. There can be at most a rank 1 subgroup of p-division points. A curve with p-torsion (possibly over an extension field) is termed *ordinary*: a curve with no p-torsion is *supersingular*. An equivalent definition is that a curve is supersingular iff p divides t. A further characterisation is in terms of the endomorphism ring already described: we note that every elliptic curve over a finite field has Frobenius as a non-trivial endomorphism.

•A supersingular curve is defined over $\mathrm{GF}(p^2)$. If defined over $\mathrm{GF}(p)$ it has $p + 1$ points. □

Schoof [27] gives an algorithm for determining the order of an elliptic curve over a finite field which runs in polynomial time, $\mathrm{O}((\log q)^8)$. The algorithm determines t modulo l for many small primes l by looking at the effect of the Frobenius automorphism on the l-division points, working in the extension of the field defined by the l-division polynomials.

Originally thought impractical, it has been successfully implemented by Atkin[4] and Elkies. Couveignes and Morain [8] give an improved version: see also Lehmann, Maurer, Müller and Shoup [20], who computed the number of points on the elliptic curve $Y^2 = X^3 + 9051969X + 11081969$ modulo the prime $10^{374} + 169$ in 1700 MIPS-days[5] (not including precomputation of the division polynomials): details are given in [3]. Morain reports[6] finding the number of points on the curve $Y^2 = X^3 + 4589X + 91228$ modulo the prime $10^{499} + 153$ in the equivalent of 4200 hours on DEC 3000 and DEC Alpha.

Atkin proposes a method of constructing elliptic curves of prescribed order modulo p by considering values of t with $d = t^2 - 4p$ small. These correspond to reduction of complex multiplication curves of discriminant d. For example, if $p \equiv 1 \bmod 4$, then it is known that p is expressible in the form $a^2 + b^2$. The elliptic curve $Y^2 = X^3 + X$ has $N_p = p + 1 - t$ where t is one of $\pm a$ or $\pm b$. (If $p \equiv 3 \bmod 4$, then this curve is always supersingular).

Complex multiplication curves: $-d = 1, 2, 3, 7, 11, 19, 43, 67, 163$ (also $-d = 1, 3, 7$ with conductor 2, $d = -3$ with conductor 3). The j-invariants are x^3 for $x = 2^2.3, 2^2.5, 0, -3.5, -2^5, -2^5.3, -2^6.3.5, -2^5.3.5.11, -2^6.3.5.23.29$ and $j = 2^3.3^3.11^3, 2^4.3^3.5^3, 3^3.5^3.17^3, -3.2^15.5^3$.

Reference to Kaltofen and Yui [15].

[2]The trace of Frobenius acting as a linear map on the *Tate module* $T_l(E)$, the inverse limit of the points of l-power order.

[3]An example of the "Riemann hypothesis for finite fields".

[4]Not published, but circulated to the NMBRTHRY electronic mailing list, 1988–1992

[5]Conventionally 1 MIPS is the power of a VAX-11/780.

[6]Electronic mail to NMBRTHRY list, 27 Jan 1995

Menezes, Vanstone, Zuccherato [24] give a version of Schoof's algorithm in the case of characteristic 2. For other methods see Lay and Zimmer [19], and Lercier and Morain [21], [25]. Koblitz [17] discusses the question of elliptic curves with prime order.

Something about twisting.

1.4 Singular curves

We defined an elliptic curve to be non-singular: that is, there is a tangent defined everywhere. If we allow a singular point, say at the origin of co-ordinates $(0,0)$, then the equation of the curve can be put (in characteristic not 2 or 3) in the form $Y^2 = X^3 + sX^2$. If $s \neq 0$ then the singular point is a *node* and there are two tangent lines $Y = \pm\sqrt{s}$: if $s = 0$ the singular point is a *cusp*.

It remains true that the non-singular points form a group. We can parametrise the points on the curve by the lines through $(0,0)$ and find that there is a bijection between the non-singular points and the points on a projective line.

•Over GF (p) the group on the non-singular points of a singular cubic $Y^2 = X^3 + sX^2$ is explicitly isomorphic to the additive GF $(p)^+$ if $s = 0$, the multiplicative group GF $(p)^*$ if s is a non-zero square and the corational group if s is not a square. □

1.5 Other curves

The construction of the group law generalises to form the *Jacobian* of a curve of higher genus. We define a *divisor* on a a curve C to the a formal finite sum of points with integer coefficients, $\sum_P n_P[P]$ and the *degree* of a divisor to be the sum of the coefficients. The divisor of a function f on C is $(f) = \sum_P d_P[P]$ where d_P is the order of the zero of f or minus the order of the pole of f at P (so d_P is zero except at finitely many points). We call these divisors *principal* and note that principal divisors have degree zero.

The *Jacobian* $J(C)$ is the group of degree zero divisors modulo principal divisors. The construction should be thought of as analogous to that of the ideal class group for a ring of algebraic integers.

•The Jacobian of a curve C of genus g has the structure of projective algebraic variety of dimension g. An elliptic curve is its own Jacobian. □

This theorem states that Jacobians are examples of *Abelian varieties*, projective varieties with a group structure (necessarily Abelian): there is a sense in which they are the only examples.

The map $P \mapsto [P] - [\mathcal{O}]$ maps an elliptic curve E to its Jacobian. If P, Q, R are collinear on E, then the (linear) function defining the line joining them has divisor $[P] + [Q] + [R] - 3[\mathcal{O}]$. (This provides an easy proof of the associativity of the group law on E.)

A curve with equation $Y^2 = f(X)$, for f a polynomial of degree d with no repeated roots, defines a curve of genus $\lfloor \frac{d-1}{2} \rfloor$. Such curves are *hyperelliptic*: every curve of genus 1 or 2 is of this form, but not every curve of higher genus is hyperelliptic.

The explicit group law on the Jacobians of curves of genus 2 has recently been worked out by Flynn [11], [12] and Cassels [6].

In the special case of hyperelliptic curves over a field of rational functions $F(X)$ there is an interpretation of the group law in terms of equivalence classes of binary quadratic forms with coefficients in the polynomial ring $F[X]$ having discriminant $f(X)$.

There is an analogue of the Weil pairing, the *Tate pairing* on the torsion points on an arbitrary Abelian variety.

References

[1] Leonard M. Adleman and Ming-Deh A. Huang (eds.), *Algorithmic number theory*, Lecture notes in Computer Science, vol. 877, Berlin, Springer Verlag, 1994, Proceedings, first international symposium, Ithaca, NY, May 1994.

[2] Bryan J. Birch, *How the number of points on an elliptic curve over a fixed prime field varies*, J. London Math. Soc. **43** (1968), 57–60.

[3] Johannes Buchmann, Volker Müller, and Victor Shoup, *Distributed computation of the number of points on an elliptic curve over a finite prime field*, Tech. Report SFB 124-TP D5 Report 03/95, April 1995.

[4] J.W.S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Maths Soc. **41** (1966), 193–291.

[5] ———, *Elliptic curves*, LMS student texts, vol. 24, Cambridge University Press, 1991.

[6] ———, *Jacobians in genus 2*, Math. Proc. Cambridge Philos. Soc. **114** (1993), no. 1, 1–8.

[7] Henri Cohen, *A course in computational number theory*, Graduate texts in mathematics, vol. 138, Springer Verlag, Berlin, 1993, Errata at `ftp://megrez.ceremab.u-bordeaux.fr/pub/cohenbook`.

[8] J.-M. Couveignes and François Morain, *Schoof's algorithm and isogeny cycles*, In Adleman and Huang [1], Proceedings, first international symposium, Ithaca, NY, May 1994, pp. 43–58.

[9] D.W. Davies (ed.), *Advances in cryptology* — EUROCRYPT *'91*, Lecture notes in Computer Science, vol. 547, Berlin, Springer, 1991.

[10] J. Fitch (ed.), *Eurosam 84*, Lecture notes in Computer Science, vol. 174, Berlin, Springer, 1984.

[11] E. Victor Flynn, *Curves of genus two*, Ph.D. thesis, University of Cambridge, ???

[12] ———, *The group law on the jacobian of a curve of genus 2*, J. Reine Angew. Math. **439** (1993), 45–69.

[13] Louis C. Guillou and Jean-Jacques Quisquater (eds.), *Advances in cryptology* — EUROCRYPT *'95*, Lecture notes in Computer Science, vol. 921, Berlin, Springer–Verlag, 1995.

[14] Dale Husemöller, *Elliptic curves*, Graduate texts in mathematics, vol. 111, Springer, New York, 1987.

[15] E. Kaltofen and N. Yui, *Explicit construction of the hilbert class fields of imaginary quadratic fields with class numbers 7 and 11*, In Fitch [10], pp. 310–320.

[16] Anthony W. Knapp, *Elliptic curves*, Princeton University Press, 1992, 0-691-08559-5.

[17] Neal Koblitz, *Primality of the number of points on an elliptic curve over a finite field*, Pacific Journal of Mathematics **131** (1988), 157–165.

[18] Kenji Koyama and Yukio Tsuruoka, *A signed binary window method for fast computing over elliptic curves*, IEICE Trans. Fund. Electron. Comm. Comp. Sci. **E76-A** (1993), 55–62, **LOOK THIS UP!**

[19] Georg-Johan Lay and Horst G. Zimmer, *Constructing elliptic curves with given group orders over large finite fields*, In Adleman and Huang [1], Proceedings, first international symposium, Ithaca, NY, May 1994, pp. 250–263.

[20] F. Lehmann, M. Maurer, V. Müller, and V. Shoup, *Counting the number of points on elliptic curves over finite fields of characteristic greater than three*, In Adleman and Huang [1], Proceedings, first international symposium, Ithaca, NY, May 1994, pp. 60–70.

[21] Reynald Lercier and François Morain, *Counting the number of points on elliptic curves over finite fields: strategies and performances*, In Guillou and Quisquater [13], pp. 79–94.

[22] James F. McKee, *Some elliptic curve algorithms*, Ph.D. thesis, University of Cambridge, 1993.

[23] ———, *Computing division polynomials*, Math. Comp. **63** (1994), no. 208, 767–771.

[24] Alfred J. Menezes, Scott A. Vanstone, and R.J. Zuccherato, *Counting points on elliptic curves over* F_{2^m}, Math. Comp. **60** (1993), 407–420.

[25] François Morain, *Building cyclic elliptic curves modulo large primes*, In Davies [9], pp. 328–336.

[26] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, *An introduction to the theory of numbers*, fifth ed., John Wiley, New York, 1991.

[27] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44** (1985), no. 170, 483–494.

[28] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate texts in mathematics, vol. 106, Springer, Berlin, 1986.