NUMBER THEORY (MICHAELMAS 1995)

Problem Sheet 1

(1) Prove that 2 is a primitive root modulo 3^n (for every $n \geq 1$).

(2) For a given $n \geq 1$, determine all possible orders of elements in $(\mathbf{Z}/3^n\mathbf{Z})^*$ and numbers of elements of a given order.

(3) (a) For $n \geq 1$, determine the exponent of $(\mathbf{Z}/6^n\mathbf{Z})^*$ (i.e. the smallest integer $d > 0$ such that $x^d \equiv 1 \pmod{6^n}$ holds for all integers x, relatively prime to 6).

(b) Prove: If $gcd(a,6) = gcd(b,6) = gcd(c,6) = 1$ and $x \equiv y \pmod 2$, then

$$a^{\left(b^{(c^x)}\right)} \equiv a^{\left(b^{(c^y)}\right)} \pmod{6^3}$$

(4) For $n \geq 1$, compute the number of solutions of the congruence

$$x^{(10^n)} \equiv 1 \pmod{10^{2n}}$$

(5) Let $n = p_1 \cdots p_k$ be a product of distinct prime numbers p_i. Prove that the following conditions are equivalent:

(a) Every integer a with $gcd(a,n) = 1$ satisfies $a^{n-1} \equiv 1 \pmod n$.

(b) $p_i - 1$ divides $n - 1$ (for every $i = 1, \ldots, k$).

(c) Every integer a satisfies $a^n \equiv a \pmod n$.

(6) Find all integers n of the form $n = 3pq$ (with $p > q > 3$ prime numbers) which satisfy the equivalent conditions in (5).

(7)* Given a prime number $r > 2$, show that there are only finitely many integers n of the form $n = pqr$ (with $p > q > r$ prime numbers) which satisfy the equivalent conditions in (5).

(8) Let p be a prime number. Prove that, for every integer $n > 0$,

$$\sum_{x=1}^{p} x^n \equiv \begin{cases} 0 \pmod p, & \text{if } (p-1) \nmid n \\ -1 \pmod p, & \text{if } (p-1) \mid n \end{cases}$$

(9) Prove: if $n \geq 1$ satisfies $2^{n-1} \equiv 1 \pmod n$, then $N := 2^n - 1$ satisfies $2^{N-1} \equiv 1 \pmod N$.

NUMBER THEORY (MICHAELMAS 1995)

Problem Sheet 2

(1) For $n \geq 1$, define

$$\Lambda(n) := \begin{cases} \log(p), & \text{if } n = p^k \text{ is a power of a prime number } p \\ 0, & \text{otherwise} \end{cases}$$

Prove that

$$\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = -\frac{\zeta'(s)}{\zeta(s)}$$

(2) Let $n > 1$ be an odd integer. Prove:

(a) If a prime number p divides $n^2 + 4$, then $p \equiv 1, 5 \pmod 8$.
(b) If a prime number p divides $n^2 + 2$, then $p \equiv 1, 3 \pmod 8$.
(c) If a prime number p divides $n^2 - 2$, then $p \equiv 1, 7 \pmod 8$.

(3) Using (2), prove that there are infinitely many prime numbers p satisfying (a) $p \equiv 5 \pmod 8$; (b) $p \equiv 3 \pmod 8$; (c) $p \equiv 7 \pmod 8$.

(4) Let $p > 2$ be a prime number, $a > 1$ an odd number. Put $b := (a^{2p} + 1)/(a^2 + 1)$. Prove:

(a) If q is a prime dividing b, then $q \equiv 1 \pmod 4$ and $q \equiv 0, 1 \pmod p$. (Hint: consider the order of $a \pmod q$.)

(b) There are infinitely many prime numbers $q \equiv 1 \pmod{4p}$.

(5) Prove: If p is a prime number dividing $2^{2^k} + 1$ (for $k \geq 1$), then

(a) $p \equiv 1 \pmod{2^{k+1}}$. (Hint: consider the order of $2 \pmod p$.)
(b) $p \equiv 1 \pmod{2^{k+2}}$. (Hint: look at the value of the Legendre symbol $\left(\frac{2}{p}\right)$.)

(6) For $k \geq 1$, let $n = 2^{2^k} + 1$. Prove:

(a) If n is a prime number, then 3 is a primitive root modulo n.
(b) If n is not a prime number, then $3^{(n-1)/2} \not\equiv -1 \pmod n$.
(c) n is a prime number if and only if $3^{(n-1)/2} \equiv -1 \pmod n$.

(7) Find the continued fraction expansion of $\sqrt{d}$ and the minimal solutions of $x^2 - dy^2 = \pm 1$ $(x, y \geq 1)$ for $d = 13, 23$.

(8) Let $a, b \geq 1$ be integers. Which real number α has a continued fraction expansion

$$\alpha = [a, b, a, b, a, b, \ldots] \qquad ?$$

NUMBER THEORY (MICHAELMAS 1995)

Problem Sheet 3

In the problems (1)–(3), $p > 2$ is a prime number.

(1) Prove: for an integer b not divisible by p, the congruence $y^2 \equiv x^2 + b \pmod{p}$ has $(p-1)$ solutions $(x, y) \in \mathbf{F}_p \times \mathbf{F}_p$. (Hint: $y^2 - x^2 = (y+x)(y-x)$.)

(2) Prove: for a polynomial $P(x)$ with integral coefficients, the number of solutions $(x, y) \in \mathbf{F}_p \times \mathbf{F}_p$ of the congruence $y^2 \equiv P(x) \pmod{p}$ is equal to

$$p + \sum_{x \in \mathbf{F}_p} \left(\frac{P(x)}{p} \right)$$

(Hint: consider first the congruence $y^2 \equiv a \pmod{p}$.)

(3) Prove: for integers a, b not divisible by p, the number of solutions $(x, y) \in \mathbf{F}_p \times \mathbf{F}_p$ of the congruence $y^2 \equiv ax^2 + b \pmod{p}$ is equal to $p - \left(\frac{a}{p}\right)$. (Hint: combine (1) and (2).)

(4) Let $p \neq q$ be prime numbers. Show that $n = pq$ is a pseudoprime with respect to the base b if and only if $b^{gcd(p-1,q-1)} \equiv 1 \pmod{n}$.

(5) Assume that $n \geq 1$ is a pseudoprime with respect to the base 2. Prove that $N := 2^n - 1$ is:
 (a) A strong pseudoprime with respect to the base 2.
 (b) An Euler pseudoprime with respect to the base 2.

(6) Let $b \in (\mathbf{Z}/341\mathbf{Z})^*$ $(341 = 11 \cdot 31)$. Prove:
 (a) 341 is a pseudoprime with respect to the base $b \iff b^{10} \equiv 1 \pmod{341} \iff b^{10} \equiv 1 \pmod{31}$.
 (b) 341 is an Euler pseudoprime with respect to the base $b \iff b^{10} \equiv 1 \pmod{341}$ and $\left(\frac{b}{11}\right) = \left(\frac{b}{31}\right) \iff b^{10} \equiv 1 \pmod{31}$ and $\left(\frac{b}{11}\right) = \left(\frac{b}{31}\right)$.
 (c) 341 is a strong pseudoprime with respect to the base $b \iff b^5 \equiv \pm 1 \pmod{341}$.
 (d) 341 is an Euler pseudoprime with respect to the base $b \iff$ 341 is a strong pseudoprime with respect to the base b.

(7) Using (6), compute the number of bases $b \in (\mathbf{Z}/341\mathbf{Z})^*$, with respect to which 341 is a preudoprime (resp. a strong pseudoprime).

(8) Prove that, for every pair of integers $p, q \in \mathbf{Z}$ $(q \neq 0)$, the following inequality holds:

$$\left| \frac{p}{q} - \sqrt{5} \right| \geq \frac{1}{(\sqrt{5}+2)q^2}$$

(Hint: distinguish three cases $p/q > \sqrt{5}$; $2 \leq p/q < \sqrt{5}$; $p/q < 2$.)