Math 445 Number Theory

Topics for the first exam

An integer p is *prime* if whenever $p = ab$ with $a, b \in \mathbb{Z}$, either $a = \pm p$ or $b = \pm p$.
[For sanity's sake, we will take the position that primes should <u>also</u> be ≥ 2 .]

Primality Tests.

How do you decide if a number n is prime?

Brute force: try to divide every number (better: prime) $\leq n$ (better $\leq \sqrt{n}$) into n, to locate a factor.

Fermat's Little Theorem. If p is prime and $(a,p) = 1$, then $a^{p-1} \equiv 1 (\text{mod } p)$.

A composite number n for which $a^{n-1} \equiv 1 (\text{mod } n)$ is called a *pseudoprime to the base a.* A composite number which is a pseudoprime to every base a satisfying $(a,n) = 1$ is called a *Carmichael number.*

$\phi(n)$ = number of integers a between 1 and n with $(a,n) = 1$; if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the prime factorization of n, then $\phi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1)$

*Euler's Theorem.*If $(a,n) = 1$, then $a^{\phi(n)} (\text{mod } n)$.

Wilson's Theorem. p is prime $\Leftrightarrow$ $(p-1)! \equiv -1 (\text{mod } p)$

Fermat $\Rightarrow$ if $(a,n) = 1$ and $a^{n-1} \not\equiv 1 (\text{mod } n)$ then n is **not** prime.

If p is prime and $a^2 \equiv 1 (\text{mod } p)$, then $a \equiv \pm 1 (\text{mod } p)$

(Miller-Rabin Test.) Given n, set $n - 1 = 2^k d$ with d odd. Then if n is prime and $(a,n) = 1$, either $a^d \equiv 1 (\text{mod } n)$ or $a^{2^i d} \equiv -1 (\text{mod} n)$ for some $i < k$.

If n is *not* prime, but the above still holds for some a, then n is called a *strong pseudoprime to the base a.*

Compositeness test: If $a^d \not\equiv \pm 1 (\text{mod } n)$, compute $a^{2^i d} (mod n)$ for $i = 1, 2, \dots$. If this sequence hits 1 **before** hitting -1, or is not 1 for $i = k$, then n is **not** prime.

Fact: If n is composite, then it is a strong pseudoprime for *at most* $1/4$ th of the a's between 1 and n.

Finding Factors.

(Pollard Rho Test.) Idea: if p is a factor of N, then for any two randomly chosen numbers a abd b, p is more likely to divide $b - a$ than N is.

Procedure: given N, use Miller-Rabin to make sure it is composite! Then pick a fairly random starting value $a_1 = a$, and a fairly random polynomial with integer coefficients $f(x)$ (such as $f(x) = x^2 + b$), then compute $a_2 = f(a_1), \dots, a_n = f(a_{n-1}), \dots$. Finally, compute $(a_{2n} - a_n, N)$ for each n. If this is > 1 and $< N$, stop: you have found a proper factor of N. If it gives you N, stop: the test has failed. You should restart with a different a and/or f.

Basic idea: this will typically find a factor on a timescale on the order of $\sqrt{p} \leq N^{1/4}$, where p is the smallest (but unknown!) prime factor of N.

RSA cryptosystem:

To send and receive messages securely: start by choosing two large primes p, q , set $n = pq$, and choose an e relatively prime to $(p-1)(q-1)$. Publish n and e. Privately compute d with $de - x(p-1)(q-1) = 1$. To send you a message, we convert the message to a number A (cutting it into blocks shorter than n if necessary), compute $B = A^e \pmod n$ and send B. You then compute (because of Euler's Theorem!) $A = B^d \pmod n$.

The security of the system rests on the fact that, to the best of our current knowledge, the fastest way to recover A from B is to determine d (in order to do *your* calculations), which seems to require knowing $(p-1)(q-1)$, which amounts to knowing p and q, which means factoring n, which is *hard*!

Periods of repeating fractions.

For integers n with $(10, n) = 1$, the fractions a/n have a repeating decimal expansion. E.g, $2/3 = .6666\ldots$, $1/7 = .142857142857\ldots$, etc.

Determining the length of the *period* (repeating part) can be done via FLT: $1/7 = .142857142857\ldots$ means $1/7 = 142857/10^6 + 142857/10^{12} + \ldots = 142857/(10^6 - 1)$, i.e $7|10^6 - 1$, and 6 is the smallest power for which this is true.

In general (if $(a, n) = 1$), we define $ord_n(a) = k =$ the smallest positive number with $a^k \equiv 1 (\text{mod } n)$. Equivalently, it is the largest number satisfying $a^r \equiv 1 (\text{mod } n) \Rightarrow ord_n(a)|r$. (Therefore, $ord_n(a)|\phi(n)$, by Euler's Theorem.)

Generally, then, the period of $1/n = ord_n(10)$, when $(10, n) = 1$. When $(10, n) > 1$, we can write $n = 2^r 5^s b = ab$ with $(10, b) = 1$, and then write

$\dfrac{1}{n} = \dfrac{1}{ab} = \dfrac{A}{a} + \dfrac{B}{b}$ for some integers A, B .

A/a will have a terminating decimal expansion, so $1/n$ will have some garbage at the beginning , and then repeat with period equal to the period of b.

Gauss conjectured that there are infinitely many primes p whose period is $p - 1$; this is still unproved.

Primality tests for special cases.

(Lucas' Theorem.) If for, each prime p with $p|n-1$, there is an a with $a^{n-1} \equiv 1 (\text{mod } n)$ but $a^{(n-1)/p} \not\equiv 1 (\text{mod } n)$, then n is prime.

Application: look at $N = 2^k + 1$. This *could* be prime only if $k = 2^n$; otherwise $k = 2^n d$, d odd, and then $2^{2^n} + 1 | (2^{2^n})^d + 1 = N$. The numbers $F_n = 2^{2^n} + 1$ are called *Fermat numbers*; the ones which are prime are called *Fermat primes*. The only known Fermat primes correspond to $n = 0, 1, 2, 3, 4$; Euler showed that $641|F_5$, and F_n is known to be composite for $n = 5, \ldots, 28$. By Lucas' Thm, F_n is prime $\Leftrightarrow$ there is an a with

$a^{F_n - 1} \equiv 1 (\text{mod } F_n)$, but $a^{(F_n-1)/2} \not\equiv 1 (\text{mod } F_n)$ (which really together means $a^{(F_n-1)/2} \equiv -1 (\text{mod } F_n)$)

Pepin showed that it if some a will work, then $a = 3$ will work!

Fermat primes are important in Euclidean geometry; Gauss showed that a regular N-sided polygon can be constructed with compass and straight-edge $\Leftrightarrow$ N is a power of 2 times a product of *distinct* Fermat primes.

Primitive roots.

A number a is called a *primitive root of 1 mod n* if $ord_n(a) = \phi(n)$ (the largest it could be).

Strong converse to Lucas' Thm: If n is prime, then there is a primitive root of 1 mod n (i.e., there is *one* a that will work for every prime p in Lucas' Thm).

The proof uses the important

(*Lagrange's Theorem.*) If p is a prime, and $f(x) = a_n x^n + \cdots a_1 x + a_0$ is a polynomial with integer coefficients, $a_n \not\equiv 0 (\text{mod } p)$, then the equation

$$f(x) \equiv 0 (\text{mod } p)$$

has at most n solutions.

This implies that if p is prime and $d|p-1$, then the equation $x^d \equiv 1 (\text{mod } p)$ has *exactly* d solutions.

Finding a primitive root mod p a prime: for each prime $p_i|p-1$, find a_i with $a_i^{(p-1)/p_i} \not\equiv 1$ (mod p), then set $a =$ the product of the a_i.

Lemma: If $ord_n(a) = m$, then $ord_n(a^k) = m/(m,k)$

Corollary: If p is prime, then there are exactly $\phi(p-1)$ (incongruent mod p) primitive roots of 1 mod p: find one, a, then the rest are a^k for $1 \leq k \leq p$ and $(k, p-1) = 1$.

Pythagorian triples:

If $a^2 + b^2 = c^2$, then we call (a, b, c) a Pythagorean triple. If $(a, b) = 1$ then $((a, c) = (b, c) = 1$ and) we call the triple *primitive*. For a primitive triple, c must be odd, a (say) even and b odd. Then because

Proposition: If $(x, y) = 1$ and $xy = c^2$, then $x = u^2, y = v^2$ for some integers u, v .

we can write $a = 2uv$, $b = u^2 - v^2$, and $c = u^2 + v^2$ for some integers u, v ; these formulas describe *all* primitive Pythagorean triples.

Sums of squares.

If $n = a^2 + b^2$, then $n \equiv 0, 1,$ or $2 (\text{mod } 4)$. Since the product of the sum of two squares

$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 = (ad + bc)^2 + (ac - bd)^2$

is the sum of two squares, and

$2n = (a^2 + b^2) \Rightarrow n = (\dfrac{a-b}{2})^2 + (\dfrac{a+b}{2})^2$ and $m = (a^2 + b^2) \Rightarrow 2m = (a-b)^2 + (a+b)^2$

it suffices to focus on odd numbers, and (more or less) odd primes.

If $p \equiv 1 (\text{mod } 4)$ is prime, then p is the sum of two squares.

If $p \equiv 3 (\text{mod } 4)$ is prime and $p|a^2 + b^2$, then $p|a$ and $p|b$.

Together, these imply that a positive integer n can be expressed as the sum of two squares $\Leftrightarrow$ in the prime factorization of n, every prime congruent to 3 mod 4 appears with even (possibly 0) exponent.

n^{th} **roots modulo a prime:.**

If p is prime and $(a, p) = 1$, then (setting $r = (n, p-1)$ the equation $x^n \equiv a (\text{mod } p)$ has

r solutions if $a^{(p-1)/r} \equiv 1 (\text{mod } p)$

no solution if $a^{(p-1)/r} \not\equiv 1 (\text{mod } p)$

This result does not really require p to be prime, only that there be a primitive root mod p. The exact statement is:

If there is primitive root of 1 mod N and $(a, N) = 1$, then (setting $r = (n, \phi(N))$ the equation $x^n \equiv a(\text{mod } N)$ has

r solutions if $a^{\phi(N)/r} \equiv 1(\text{mod } N)$
no solution if $a^{\phi(N)/r} \not\equiv 1(\text{mod } N)$

For example, every odd prime power p^k has a primitive root. In fact, if b is a primitive root mod p, then all but at most one of $b + kp, 0 \leq k \leq p - 1$ is a primitive root mod p^2 ; and if b is a primitive root mod p^2, then it is a primitive root mod p^k for all $k \geq 2$.

(Euler's Criterion.) The equation $x^2 \equiv a(\text{mod } p)$ has a solution ($p =$ odd prime) $\Leftrightarrow a^{(p-1)/2} \equiv 1(\text{mod } p)$; it then has two solutions (x and $-x$).

The equation $x^2 \equiv -1(\text{mod } p)$ has a solution $\Leftrightarrow (-1)^{(p-1)/2} \equiv 1(\text{mod } p) \Leftrightarrow p = 2$ or $p \equiv 1(\text{mod } 4)$

If f is a polynomial with integer coefficients and $(M, N) = 1$, then the congruence equation $f(x) \equiv 0 \pmod{MN}$ has a solution $\Leftrightarrow$ the equations $f(x) \equiv 0 \pmod{M}$ and $f(x) \equiv 0 \pmod{N}$ both do.

In particular, for $f(x) =$ a polynomial with integer coefficients, let $S(n) =$ the number of (incongruent, mod n) solutions to the congruence equation $f(x) \equiv 0(\text{mod } n)$. Then:

If $(M, N) = 1$, then $S(MN) = S(M) \times S(N)$. The obvious generalization follows by induction. So: to decide if a congruence equation has a solution (and how many), it suffices to decide this for the prime power factors of the modulus. So we can, for example, decide if $x^n \equiv a \pmod{N}$ has any solutions (and how many) for every odd N and $(a, N) = 1$. Some day we should handle powers of 2, too....