Today's Outline

Review

More examples of Miller-Rabin strong-pseudoprime test

Euler's criterion for e^{th} roots modulo primes $p = 1 \bmod e$

Primitive roots modulo primes

Euler's phi function

Review

• Be able to distinguish *reduction modulo* m from *equality modulo* m.

$$a = b \bmod m \quad \text{means} \quad m|(a-b)$$

$a \,\%\, m =$ remainder when a is divided by m

Yes, always

$$(a \,\%\, m) = a \bmod m$$

and also

$$a = (a \,\%\, m) \bmod m$$

• **Notation:** $\mathbf{Z}/m = \{\text{integers mod } m\}$

$$\mathbf{Z}/m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$$

• Fast Modular Exponentiation algorithm.

• Fermat's Little Theorem (special case of Euler's theorem).

• Formula for square roots for prime $p = 3 \bmod 4$ with mandatory checking.

• Easy formula for e^{th} roots mod prime p for e prime, $p \neq 1 \bmod e$. (*Everything* is an e^{th} power modulo such p.)

• Less easy formula for e^{th} roots mod prime p for e prime, $p = 1 \bmod e$, $e^2 \not| (p-1)$, with mandatory checking.

• Fermat pseudoprime tests. Only moderately good, but very cheap/feasible.

Miller-Rabin test, Strong Pseudoprimes

Again: For odd integer n factor

$$n - 1 = 2^s \cdot \ell$$

with ℓ odd. Then n is a **strong pseudoprime base** b if

$$b^\ell = 1 \bmod n$$

or if for some $0 \leq r < s$

$$b^{2^r \cdot \ell} = -1 \bmod n$$

If n fails the test for some b, then n is **definitely composite**.

The heuristic is that if n *passes* base b then the **probability is at least** $3/4$ **that** n **is prime.**

(strong pseudoprime base b implies Fermat pseudoprime base b.)

Miller-Rabin test base b:
factor $n-1 = 2^s \cdot m$ with m odd
replace b by $b^m \bmod n$
    if $b = \pm 1 \bmod n$ **stop:** n is 3/4 prime
    else continue
set $r = 1$
while $r < s$
    replace b by $b^2 \bmod n$
    if $b = -1 \bmod n$ **stop:** n is 3/4 **prime**
    elsif $b = +1 \bmod n$ **stop:** n is **composite**
    else replace r by $r + 1$ and **continue**
if we fall out of the loop, n is **composite**.

If n passes this test it is a **strong pseudoprime base** b. The conclusion that n is **composite** always means *definitely* composite. The conclusion of **prime** really is just **pseudoprime** or **probable prime**.

If n is a strong pseudoprime base b, then b is a **witness** to the primality of b. If n is *not* prime, then b is a **false witness**.

Miller-Rabin test base 2 on 111

Factor $111 - 1 = 2^s \cdot m$ with m odd: here $m = 55$ and $s = 1$.

(By fast exponentiation) replace $b = 2$ by $b^m \bmod 111 = 2^{55} = 35 \bmod 111$.

Since $b = 35 \neq \pm 1 \bmod 111$ we continue, entering the squaring loop. Set $t = 1$.

Since $t = 1 = s$, we fall out of the squaring loop: 111 is not a strong pseudoprime base 2. (So it is definitely composite.)

Note that we did *not* find a factor of 111, but we know it is composite.

Miller-Rabin test base 2 on 113

Factor $113 - 1 = 2^s \cdot m$ with m odd: here $m = 7$ and $s = 4$.

Then (using the fast exponentiation algorithm) replace $b = 2$ by $b^m \bmod 113 = 2^7 = 15 \bmod 113$.

Since $b = 15 \neq \pm 1 \bmod 113$ we continue, entering the squaring loop. Set $t = 1$.

Replace $b = 15$ by $b^2 = 15^2 = 112 \bmod 113$.

Since $b = 112 = -1 \bmod 113$ we conclude that 113 is a strong pseudoprime base 2.

Miller-Rabin test base 2 on 1001

Factor $1001 - 1 = 2^s \cdot m$ with m odd: here $m = 125$ and $s = 3$.

(By fast exponentiation algorithm) $b = 2$ by $b^m \bmod 1001 = 2^{125} = 32 \bmod 1001$.

Since $b = 32 \neq \pm 1 \bmod 1001$ we continue, entering the squaring loop. Set $t = 1$.

Replace $b = 32$ by $b^2 = 32^2 = 23 \bmod 1001$.

This $b = 23$ is neither $\pm 1 \bmod 1001$ so continue. Increment t to 2.

Replace $b = 23$ by $b^2 = 23^2 = 529 \bmod 1001$. This $b = 529$ is neither $\pm 1 \bmod 1001$ so continue. Increment t to 3.

Since $t = 3 = s$, we fall out of the squaring loop: 1001 is not a strong pseudoprime.

(Secretly, it is $1001 = 7 \cdot 11 \cdot 13$.)

Euler's criterion for roots

This result complements our earlier formulas for roots modulo primes.

Theorem: Let e be a positive integer and p a prime with $p = 1 \bmod e$. An integer b not 0 modulo p is an e^{th} power modulo p if and only if

$$b^{\frac{p-1}{e}} = 1 \bmod p$$

Half of this is a consequence of Fermat's Little Theorem. Namely, *if* b is an e^{th} power then $b^{\frac{p-1}{e}} = 1 \bmod p$. Thus, if $b^{\frac{p-1}{e}} \neq 1 \bmod p$ then b is *not* an e^{th} power mod p.

The other half, that if $b^{\frac{p-1}{e}} = 1 \bmod p$ then b is an e^{th} power uses **primitive roots**, which we didn't yet discuss.

Yes, use **fast modular exponentiation**, of course.

Examples of Euler's criterion

Is 2 a square modulo 101? To invoke Euler's criterion, compute $2^{(101-1)/2} \,\%\, 101$ (by fast modular exponentiation), obtaining 100, which is *not* 1 mod 101. Thus, by Euler's criterion, 2 is *not* a square mod 101.

Is 2 a square modulo 103? To invoke Euler's criterion, compute $2^{(103-1)/2} \,\%\, 103$ (by fast modular exponentiation), obtaining $1 \bmod 103$. Thus, by Euler's criterion, 2 *is* a square mod 103.

Is 2 a 17^{th} power modulo 103? To invoke Euler's criterion, first observe that $103 = 1 \bmod 17$. Then compute $2^{(103-1)/17} \,\%\, 103$ (by fast modular exponentiation), obtaining $64 \neq 1 \bmod 103$. Thus, by Euler's criterion, 2 is *not* a 17^{th} power mod 103.

Note that Euler's criterion for *square roots* can be used for any prime > 2.

Proof: (of Euler's criterion).

Suppose $b = c^e \bmod p$ is an e^{th} power modulo p (with p not dividing b). Suppose that $p = 1 \bmod e$, so that $p = 1 + \ell e$ for some integer ℓ. Then

$$b^{\frac{p-1}{e}} = (c^e)^{\frac{p-1}{e}} = c^{p-1} = 1 \bmod p$$

by Fermat's Little Theorem. (The *contrapositive* is that if $b^{(p-1)/e} \neq 1 \bmod p$ then b cannot be an e^{th} power modulo p.)

The other direction of implication uses existence of a **primitive root** g modulo the prime p. We interrupt the proof of Euler's criterion to explain primitive roots modulo *primes*. Discussion of primitive roots for other moduli will have to wait a little.

Primitive roots modulo primes

A **primitive root** g modulo a prime p is an integer g relatively prime to p such that no positive exponent ℓ smaller than $p-1$ will make

$$g^{\ell} = 1 \bmod p$$

From Fermat's Little Theorem we know that $g^{p-1} = 1 \bmod p$. The content of this condition on g is that no *smaller* positive integer will make this true.

Theorem: Primitive roots modulo primes exist.

This is not easy to prove, but is a very important result.

Testing for primitive roots:

Proposition: An integer g is a primitive root modulo a prime p if, for every prime q dividing $p-1$,

$$g^{\frac{p-1}{q}} \neq 1 \bmod p$$

Proof: On one hand, if g is a primitive root no smaller positive exponent than $p-1$ will do. On the other hand, if ℓ is the smallest positive exponent with $g^{\ell} = 1 \bmod p$, let $p-1 = q \cdot \ell + r$ with $0 \leq r < \ell$. By Fermat's Little Theorem

$$1 = g^{p-1} = g^{q\ell+r} = (g^{\ell})^{q} \cdot g^{r} \bmod p$$

$$= 1^{q} \cdot g^{r} \bmod p$$

Since ℓ was the smallest positive integer with that property, $r = 0$, and ℓ divides $p-1$. Any prime q dividing $(p-1)/\ell$ will give

$$g^{\frac{p-1}{q}} = 1 \bmod p$$

as claimed. ///

Is 2 a primitive root modulo 47? By trial division 47 is a prime, so the criterion above applies. By trial division, $47 - 1 = 2 \cdot 23$. Via fast modular exponentiation

$$2^{\frac{47-1}{23}} = 2^2 \neq 1 \bmod 47$$

$$2^{\frac{47-1}{2}} = 2^{23} = 1 \bmod 47$$

so 2 is *not* a primitive root modulo 47.

Is 3 a primitive root modulo 47? Again, by trial division 47 is a prime, so the criterion above applies, and $47 - 1 = 2 \cdot 23$. Via fast modular exponentiation

$$3^{\frac{47-1}{23}} = 3^2 = 9 \neq 1 \bmod 47$$

$$3^{\frac{47-1}{2}} = 3^{23} = 1 \bmod 47$$

so 3 is *not* a primitive root modulo 47.

But if we believe the theorem there must be a primitive root, so we keep hunting. (Think why we don't try 4?!)

Is 5 a primitive root modulo 47? With the same set-up,

$$5^{\frac{47-1}{23}} = 5^2 = 25 \neq 1 \bmod 47$$

$$5^{\frac{47-1}{2}} = 5^{23} = 46 \bmod 47$$

so 5 *is* a primitive root modulo 47.

It turns out that there are $\varphi(p-1)$ primitive roots modulo p, where φ is Euler's phi-function (below), so guessing at random has chance $\varphi(p-1)/p$ of finding a primitive root, which is not so bad.

Proposition: For g a primitive root mod prime p, $1, g, g^2, g^3, \ldots, g^{p-2}$ are distinct. Any $b \neq 0 \bmod p$ is expressible as $b = g^t \bmod p$ for exactly one t with $0 \leq t \leq p-2$.

Proof: For a non-negative integer i, let $g^{-i} \bmod p$ be the i^{th} power of the multiplicative inverse of g modulo p. If

$$g^i = g^j \bmod p$$

for some $0 \leq i \leq j \leq p-2$, then multiply through by $g^{-i} \bmod p$ to obtain

$$1 = g^{j-i} \bmod p$$

Since $0 \leq j - i < p - 2$, and $p - 1$ is the smallest *positive* exponent ℓ which makes $g^\ell = 1 \bmod p$, it must be that $i = j$. This proves that these are all different. Since these are $p - 1$ different values of g^t modulo p and there are exactly $p - 1$ *equivalence classes* other than $0 \bmod p$, any $b \neq 0 \bmod p$ is expressible as $b = g^t \bmod p$ for exactly one t in that range. ///

Proposition: Let g be a primitive root modulo a prime p. For an integer ℓ, $g^\ell = 1 \bmod p$ if and only if $\ell = 0 \bmod p-1$.

Proof: On one hand, if $\ell = m \cdot (p-1)$, then

$$g^\ell = (g^{p-1})^m = 1^m = 1 \bmod p$$

On the other hand, if $g^\ell = 1 \bmod p$, use the division algorithm to express

$$\ell = q \cdot (p-1) + r$$

with $0 \leq r < p-1$. Then

$$1 = g^\ell = g^{r+q(p-1)} = g^r \cdot (g^{p-1})^q$$

$$= g^r \cdot 1^q = g^r \bmod p$$

Since g is a primitive root, $p-1$ is the smallest positive exponent m such that $g^m = 1 \bmod p$. Thus, $r = 0$, and $p-1$ divides ℓ. ///

Returning to the proof of Euler's criterion:

We want to prove that if $b^{(p-1)/e} = 1 \bmod p$ then b is an e^{th} power mod p. Using the previous proposition, let $b = g^t \bmod p$ with $0 \leq t \leq p-2$. If $b^{(p-1)/e} = 1 \bmod p$ then

$$1 = b^{(p-1)/e} = (g^t)^{(p-1)/e} = g^{t(p-1)/e} \bmod p$$

By the previous proposition, $p-1$ must divide $t(p-1)/e$. Let $t(p-1)/e = n(p-1)$. Then $t/e = n$, so $e|t$. That is

$$b = g^t = (g^{t/e})^e \bmod p$$

expressing b as an e^{th} power modulo p.

This finishes the harder half of the proof of Euler's criterion, if we grant ourselves the existence of primitive roots modulo primes.

///

Euler's φ-function

Euler's φ-function or phi-function is

$\varphi(n) =$ number of $1 \leq x \leq n$ with $\gcd(x, n) = 1$

For prime p, it is easy to see that $\varphi(p) = p - 1$.

We had observed that x has a multiplicative inverse modulo n if and only if $\gcd(x, n) = 1$, so also $\varphi(n)$ is the number of *congruence classes mod* n which have multiplicative inverses.

Clever computation of $\varphi(n)$ uses a *factorization* of n, though we can also just use brute force.

The security of RSA depends upon the difficulty of computing $\varphi(pq)$. If it were easy to compute, RSA would be broken, because an attacker could compute the decryption exponent d as the multiplicative inverse of the encryption exponent e modulo $\varphi(pq)$ without knowing p and q.

Brute force computation of $\varphi(15)$

Initialize counter $c = 0$.

Is $\gcd(1, 15) = 1$? Yes, increment to $c = 1$.

Is $\gcd(2, 15) = 1$? Yes, increment to $c = 2$.

Is $\gcd(3, 15) = 1$? No, do not increment.

Is $\gcd(4, 15) = 1$? Yes, increment to $c = 3$.

Is $\gcd(5, 15) = 1$? No, do not increment.

Is $\gcd(6, 15) = 1$? No, do not increment.

Is $\gcd(7, 15) = 1$? Yes, increment to $c = 4$.

Is $\gcd(8, 15) = 1$? Yes, increment to $c = 5$.

Is $\gcd(9, 15) = 1$? No, do not increment.

Is $\gcd(10, 15) = 1$? No, do not increment.

Is $\gcd(11, 15) = 1$? Yes, increment to $c = 6$.

Is $\gcd(12, 15) = 1$? No, do not increment.

Is $\gcd(13, 15) = 1$? Yes, increment to $c = 7$.

Is $\gcd(14, 15) = 1$? Yes, increment to $c = 8$.

Is $\gcd(15, 15) = 1$? No, do not increment.

So $\varphi(15) = 8$.

Horribly slow.

A medium good formula for $\varphi(n)$

Rather than taking n steps to compute $\varphi(n)$, a prime factorization of n gives a formula for $\varphi(n)$.

Theorem: With prime factorization of n

$$n = p_1^{e_1} \dots p_t^{e_t}$$

with the p_i distinct primes and the e_i positive integers, then

$$\varphi(n) = (p_1 - 1)p_1^{e_1 - 1} \dots (p_t - 1)p_t^{e_t - 1}$$

Since factorization takes at worst $\sqrt{n}$ steps, this formula is much better than brute force, but is still **infeasible** for $n \sim 10^{100}$, since we cannot expect to factor n of that size.