

Congruences, continued

Definition: A set of m integers r_1, \dots, r_m is a *complete set of residues (CSR) modulo m* if every integer is congruent \pmod{m} to exactly one of the r_i 's.

Examples: $\{0, \dots, m - 1\}$ and all integers between $-m/2$ and $m/2$ (including one of them if m is even) are two CSR's modulo m .

$\{-10, 91, -3, 13, 109\}$ is a CSR modulo 5.

Theorem: Let a, b, c, d, x, y, m and n be integers with m and n greater than 1. Then

(a) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ax \pm cy \equiv bx \pm dy \pmod{m}$.

(b) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

(c) If $f(x)$ is a polynomial with integer coefficients and $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$.

(d) If $a \equiv b \pmod{m}$ and $n|m$, then $a \equiv b \pmod{n}$.

Clock arithmetic is arithmetic modulo 12 or 24.

Addition, subtraction and multiplication of numbers modulo m work just like these operation on integers.

However, division does not always work as for integers:

$$2 \cdot 3 = 6 \equiv 18 = 2 \cdot 9 \pmod{12},$$

but $3 \not\equiv 9 \pmod{12}$.

In general $ac \equiv bc \pmod{m}$ does not always imply $a \equiv b \pmod{m}$.

Definition: The *greatest common divisor* (or GCD) of two positive integers is the largest integer which divides both of them.

Definition: Two positive integers are *relatively prime* if their GCD is 1.

Lemma. If $\gcd(a, m) = 1$ and $0 \leq i < j < m$, then $ai \not\equiv aj \pmod{m}$.

Proof. If not, then $m|a(i-j)$. Since $\gcd(a, m) = 1$, we have $m|(i-j)$, which contradicts the bounds on i and j .

Theorem. If $\gcd(a, m) = 1$, then there is an x in $0 < x < m$ such that $ax \equiv 1 \pmod{m}$.

Proof. By the Lemma, the set

$$\{ai \pmod{m}; i = 1, \dots, m-1\}$$

is a permutation of $\{1, \dots, m-1\}$. Therefore 1 is in this set (the first one).

Note: The x in this Theorem is like “ a^{-1} ”

Now we can say when we can divide in congruences:

Theorem. If $m > 1$, a , b , c are integers, ($c \neq 0$), $\gcd(c, m) = 1$, then $ac \equiv bc \pmod{m}$ implies $a \equiv b \pmod{m}$.

Proof. By the previous Theorem, there is an x such that $cx \equiv 1 \pmod{m}$. Then $ac \equiv bc$ implies $acx \equiv bcx$ implies $a1 \equiv b1$ implies $a \equiv b \pmod{m}$.

How to solve the congruence $ax \equiv b \pmod{m}$:

Theorem. Let $m > 1$, a and b be integers. Let $g = \gcd(a, m)$. If $g \nmid b$, then $ax \equiv b \pmod{m}$ has no solution. If $g \mid b$, then it has g solutions

$$x \equiv \frac{b}{g}x_0 + t\frac{m}{g} \pmod{m}, \quad t = 0, 1, \dots, g - 1,$$

where x_0 is any solution of $\frac{a}{g}x_0 \equiv 1 \pmod{\frac{m}{g}}$.

That is,

$$x = \frac{b}{g}x_0 + t\frac{m}{g} \pmod{m}, \quad t = 0, 1, \dots,$$

are all integer solutions x .

Examples. (a) Solve $7x \equiv 3 \pmod{12}$.

$g = \gcd(7, 12) = 1$, $g|b$ since $1|3$, so there is one solution. $7 \cdot 7 \equiv 1 \pmod{12}$, so $x_0 = 7$ and the solution to $7x \equiv 3 \pmod{12}$ is $x = 3 \cdot 7 + t \cdot 12 = 21 + 12t \equiv 9 \pmod{12}$.

(b) Solve $657x \equiv 36 \pmod{963}$.

$g = \gcd(657, 963) = 9$. $g = 9|36 = b$, so there are 9 solutions. To find them, we must solve

$$\frac{657}{9}x_0 \equiv 1 \pmod{\frac{963}{9}}.$$

That is, $73x_0 \equiv 1 \pmod{107}$. We find $x_0 \equiv 22$. Then,

$$x_0 = \frac{36}{9} \cdot 22 + t \frac{963}{9} = 88 + 107t,$$

That is, $x \equiv 88 \pmod{107}$. The nine solutions of the original congruence are:

$$x \equiv 88, 88 + 107, 88 + 2 \cdot 107, \dots, 88 + 8 \cdot 107 \pmod{963}.$$

Fermat and Euler's Theorems

Definition: A *reduced set of residues* (RSR) modulo m is a set of integers R so that every integer relatively prime to m is congruent to exactly one integer in R .

Fact. $a \equiv b \pmod{m}$ implies $\gcd(a, m) = \gcd(b, m)$.

Fact. All RSR's modulo m have the same size.

Definition: $\phi(m)$ is the size of a RSR modulo m . ϕ is called the *Euler Phi* or *totient function*.

The standard CSR modulo m is $\{0, \dots, m-1\}$.

The standard RSR modulo m is $\{1 \leq r \leq m; \gcd(r, m) = 1\}$.

Fact. ϕ is *multiplicative*, that is, $\phi(ab) = \phi(a)\phi(b)$ whenever a and b are relatively prime.

Some special formulas for ϕ : Let p be prime. Then $\phi(p) = p - 1$, $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$, $\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$.

When $p \neq q$ are primes, we have $\phi(pq) = (p - 1)(q - 1)$.

Fermat's "Little" Theorem

Theorem. Let p be prime and a be an integer which is not a multiple of p . Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof: Since $\gcd(a, p) = 1$, the set $\{ai \pmod{p}; i = 1, \dots, p-1\}$ is the same as the set $\{1, \dots, p-1\}$. Therefore,

$$a^{p-1} \prod_{i=1}^{p-1} i = \prod_{i=1}^{p-1} (ai) \equiv \left(\prod_{i=1}^{p-1} i \right) \cdot 1 \pmod{p}.$$

Since $\gcd(\prod_{i=1}^{p-1} i, p) = 1$, we can cancel and get $a^{p-1} \equiv 1 \pmod{p}$.

Euler's Theorem

Theorem. Let $m > 1$ and $\gcd(a, m) = 1$.
Then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Proof: Let $\{r_1, \dots, r_{\phi(m)}\}$ be a RSR modulo m . Then $\{ar_1, \dots, ar_{\phi(m)}\}$ is a RSR modulo m , too (by a Lemma). Therefore, for all i , there is a unique j so that $r_i \equiv ar_j \pmod{m}$. Then

$$a^{\phi(m)} \prod_{i=1}^{\phi(m)} r_i = \prod_{i=1}^{\phi(m)} (ar_i) \equiv \left(\prod_{i=1}^{\phi(m)} r_i \right) \pmod{m}.$$

Since $\gcd(\prod_{i=1}^{\phi(m)} r_i, m) = 1$, we can cancel and get $a^{\phi(m)} \equiv 1 \pmod{m}$.

A Corollary of Euler's Theorem

Here is an alternate way to compute the multiplicative inverse a^{-1} of a modulo m : Recall that a^{-1} is the residue class mod m such that $a^{-1}a \equiv aa^{-1} \equiv 1 \pmod{m}$. It is defined only when $\gcd(a, m) = 1$. In that situation we have $a^{\phi(m)} \equiv 1 \pmod{m}$ by Euler's Theorem.

Factoring out one a gives

$$aa^{\phi(m)-1} \equiv 1 \pmod{m},$$

whence $a^{-1} \equiv a^{\phi(m)-1} \pmod{m}$. For a prime modulus p we have $a^{-1} \equiv a^{p-2} \pmod{p}$.

For large m , computing $a^{-1} \pmod{m}$ by this formula requires roughly the same number of bit operations as computing $a^{-1} \pmod{m}$ by the Extended Euclidean Algorithm. (The latter must be used if one does not know $\phi(m)$.)

How to compute $a^n \bmod m$ swiftly

Here is an algorithm for computing a^n in $O(\log_2 n)$ multiplications. To use it to compute $a^n \bmod m$ while keeping the numbers small (smaller than m , that is), reduce modulo m after each multiplication.

```
procedure power(a,n)
  e = n;
  y = 1;
  z = a;
  repeat {
    if (e is odd) y = y*z;
    if (e <= 1) return (y);
    z = z*z;
    e = floor(e/2);
  }
end power;
```

Another Corollary of Euler's Theorem

Corollary. Let $m > 1$, x , y and g be positive integers with $\gcd(g, m) = 1$. If $x \equiv y \pmod{\phi(m)}$, then $g^x \equiv g^y \pmod{m}$.

Proof: We have $x = y + k\phi(m)$ for some integer k , so

$$g^x = g^{y+k\phi(m)} = g^y (g^{\phi(m)})^k \equiv g^y \pmod{m}.$$

Finding large primes

Fermat's Little Theorem says that if p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

This theorem gives a test for *compositeness*: If p is odd and $p \nmid a$ and $a^{p-1} \not\equiv 1 \pmod{p}$, then p is not prime.

If the converse of Fermat's theorem were true, it would give a fast test for *primality*. The converse would say, if p is odd and $p \nmid a$ and $a^{p-1} \equiv 1 \pmod{p}$, then p is prime.

Unfortunately, this converse is not a true statement, although it is true for most p and most a . Consider $p = 341 = 11 \cdot 31$ and $a = 2$. $2^{340} \equiv 1 \pmod{341}$.

It is even worse than that because there are infinitely many *Carmichael numbers*. These are composite numbers like $p = 561 = 3 \cdot 11 \cdot 17$ for which $a^{p-1} \equiv 1 \pmod{p}$ for every integer a with $\gcd(a, p) = 1$.

Here is a true converse of Fermat's Little Theorem.

Theorem. Let $n > 3$ be odd. If for every prime $p|n-1$ there exists an a such that $a^{n-1} \equiv 1 \pmod{n}$, but $a^{(n-1)/p} \not\equiv 1 \pmod{n}$, then n is prime.

This theorem may be used iteratively to construct large, random primes.

Begin with a prime p_1 . Let $i = 1$. Repeat the following steps until p_i is large enough.

For random small integers k , let $n = 2kp_i + 1$. If $2^{n-1} \not\equiv 1 \pmod{n}$, then n is composite by Fermat's Little Theorem, so try another k . Otherwise, n is probably prime, so try to prove n is prime using the theorem just stated. Note that $n - 1 = 2kp_i$ is easy to factor completely. If you succeed in finding a 's which satisfy the conditions of the theorem, then n is proved prime, and let $p_{i+1} = n$ and let $i = i + 1$. Otherwise, try a new random k .