

Congruences

One of the fundamental tools of number theory is the congruence. This idea will be critical to most of what we do the rest of the term. This set of notes partially follows the book's treatment. I will not use the language of abstract algebra, however, to the extent that the book does. In addition, I will present some results of historical importance, which are not in the book.

Definition. We say $a \equiv b \pmod{m}$ (read "a is congruent to b modulo m") if $a - b$ is divisible by m .

If $a = qm + r$, where $0 \leq r < m$, then $a \equiv r \pmod{m}$. We refer to r as the **least residue** of a modulo m and say that a belongs to the **residue class** of r . The book denotes this $a \in \bar{r}$, where \bar{r} is the set $\{\dots, r - 2m, r - m, r, r + m, r + 2m, \dots\}$. I will not refer much to residue classes.

Theorem. Let $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then

- 1) $a + c \equiv b + d \pmod{m}$
- 2) $ac \equiv bd \pmod{m}$
- 3) for any $n > 0$, $a^n \equiv b^n \pmod{m}$.

Proof: I will leave you to prove (1). You should try to do this to get used to working with congruences. (3) follows from (2) (with $c = a$ and $d = b$). Here is a verification of (2): if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then for some integers k_1 and k_2 , $a - b = k_1m$ and $c - d = k_2m$. Writing this as $a = b + k_1m$ and $c = d + k_2m$, we have $ac = (b + k_1m)(d + k_2m) = bd + m(k_1d + k_2b + k_1k_2m)$. Thus, $ac - bd$ is a multiple of m , so $ac \equiv bd \pmod{m}$, as desired.

Division is not possible in general with congruences. For example, $24 \equiv 84 \pmod{15}$ but if we divide both sides by 6, we get $4 \equiv 14 \pmod{15}$, which is not correct. However, we do have the following:

Theorem. If $ac \equiv bc \pmod{m}$ and $(c, m) = 1$, then $a \equiv b \pmod{m}$.

More generally, if $ac \equiv bc \pmod{m}$, and $(c, m) = d$, then $a \equiv b \pmod{m/d}$.

Proof: If $ac \equiv bc \pmod{m}$, then for some integer k , $ac - bc = km$, or $(a - b)c = km$. If $(c, m) = d$, then for some integers x and y , $cx + my = d$. Now $(a - b)cx = kmx$ and $cx = d - my$ so $(a - b)(d - my) = kmx$. Dividing by d , $(a - b)\left(1 - \frac{my}{d}\right) = \frac{kmx}{d}$. Thus, $a - b = \frac{m}{d}(kx + (a - b)y)$, which means that $a \equiv b \pmod{m/d}$. If $d = 1$, we get the first assertion.

Fermat noticed that if p is prime and q is a divisor of $2^p - 1$, then $q \equiv 1 \pmod{p}$. He also noticed that $2^{p-1} \equiv 1 \pmod{p}$ whenever p is prime. We wish to verify each of these observations. The following is one of the most important theorems in computational number theory.

Theorem (Fermat's Little Theorem). If p is prime and a is any integer, then $a^p \equiv a \pmod{p}$.

Proof. The book derives this theorem as a corollary to Euler's theorem, which we state in a bit. Here is an alternative proof by induction: noticing that $(-a)^p = -a^p$, so if we can establish the result for nonnegative a , we will have it for negative a as well.

Inducting on a , the result is trivial if $a = 0$. Having established the result for a , we have

$$(a + 1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1. \text{ Now } \binom{p}{k} = \frac{p!}{k!(p-k)!},$$

and this will be divisible by p if there is no p in the denominator, which is the case if $1 \leq k \leq p - 1$. Thus, all the middle binomial coefficients are congruent to $0 \pmod{p}$. Hence, $(a + 1)^p \equiv a^p + 1 \pmod{p} \equiv a + 1 \pmod{p}$, and we have established our inductive step.

Corollary. (Also called Fermat's Little Theorem) If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

This follows by the cancellation theorem previously proved: if $p \nmid a$, then $(p, a) = 1$.

If n is not prime, then usually, $a^{n-1} \not\equiv 1 \pmod{n}$. As we will see shortly, this gives a quick way to determine if a number is not prime. For example, $2^{14} = 16384 \equiv 4 \pmod{15}$. Thus, 15 can't be prime. Unfortunately, this test is not foolproof. It turns out that $2^{340} \equiv 1 \pmod{341}$ even though $341 = 11 \cdot 31$. If a composite number n has

the property that $2^{n-1} \equiv 1 \pmod{n}$, then n is called a **base 2 pseudoprime**. These numbers are rare: there are 245 pseudoprimes less than 1,000,000 while there are 78,498 primes less than 1,000,000. So if a number, selected at random, less than a million has the property that $2^{n-1} \equiv 1 \pmod{n}$, the probability that it is prime is $\frac{78,498}{245 + 78,498}$ which is .997, pretty good odds.

Now even though 341 is a base 2 pseudoprime, it is not a base 3 pseudoprime: $3^{340} \equiv 56 \pmod{341}$. There are very rare numbers that are pseudoprimes to infinitely many bases. A number n such that $a^n \equiv a \pmod{n}$ for all integers a is called a **Carmichael number**. Carmichael was a mathematician trying to prove that such numbers did not exist. While getting properties that such numbers would have to satisfy, he discovered, in 1910, that 561 had these properties. Of course Carmichael numbers are much rarer than pseudoprimes. Of the 245 base 2 pseudoprimes less than a million, only 43 of them are Carmichael numbers. Even so, it was proved in 1993 that there are infinitely many Carmichael numbers.

A useful function for us is **Euler's phi function**: $\varphi(n)$ = the number of positive integers less than n which are relatively prime to n . For example, the numbers prime to 15 are 1, 2, 4, 7, 8, 11, 13, 14. There are 8 of these, so $\varphi(15) = 8$.

Theorem (Euler's theorem) If $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof: Let $\varphi(n) = k$. Let $x_1, x_2, x_3, \dots, x_k$ be the integers prime to n . By a previous theorem, since $(a, n) = 1$, $ax \equiv ay \pmod{n}$ only if $x \equiv y \pmod{n}$. Because of this, the numbers ax_1, ax_2, \dots, ax_k are all distinct modulo n . They are also relatively prime to n , so modulo n , they must be a reordering of x_1, x_2, \dots, x_n . This means that $x_1x_2 \cdots x_k \equiv ax_1ax_2 \cdots ax_k \pmod{n}$, or $x_1x_2 \cdots x_k \equiv a^kx_1x_2 \cdots x_k \pmod{n}$. Since $x_1x_2 \cdots x_k$ is prime to n , this term can cancel leaving us with $a^k \equiv 1 \pmod{n}$.

As the book points out, Fermat's Little Theorem is a corollary since if p is a prime, $\varphi(p) = p - 1$. As an example of Euler's theorem, if $n = 15$, then $\varphi(n) = 8$. If $a = 2$, then $2^8 = 256$, which is congruent to 1 modulo 15.

We now turn to Fermat's other observation, that if q is a prime dividing $2^p - 1$ then $q \equiv 1 \pmod{p}$. For example, $2^{11} - 1 = 2047 = 23 \cdot 89$, and both 23 and 89 are congruent to 1 mod 11. We still need one more tool.

Lemma. For any positive integers m and n , $(a^m - 1, a^n - 1) = a^{(m, n)} - 1$.

Proof. We may assume that $m \geq n$. We have $(a^m - 1, a^n - 1) = (a^m - a^n, a^n - 1) = (a^n(a^{m-n} - 1), a^n - 1)$. Since a^n is relatively prime to $a^n - 1$ (why?) it follows that $(a^n(a^{m-n} - 1), a^n - 1) = (a^{m-n} - 1, a^n - 1)$ (why?). Now suppose that $m = qn + r$. Then $m - n = (q - 1)n + r$. If we repeat the above procedure q times, we have $(a^m - 1, a^n - 1) = (a^n - 1, a^r - 1)$. This completely mimics the gcd calculation $(m, n) = (n, r)$. Consequently, after some number of steps, $(a^m - 1, a^n - 1) = (a^{(m, n)} - 1, a^0 - 1)$. But $a^0 - 1 = 0$, and $(k, 0) = k$, so $(a^m - 1, a^n - 1) = a^{(m, n)} - 1$.

For example, suppose $m = 84$ and $n = 35$. We have

$$\begin{aligned} (a^{84} - 1, a^{35} - 1) &= (a^{84} - a^{35}, a^{35} - 1) = (a^{35}(a^{49} - 1), a^{35} - 1) \\ &= (a^{49} - 1, a^{35} - 1) = (a^{14} - 1, a^{35} - 1) = (a^{35} - 1, a^{14} - 1) \\ &= (a^{21} - 1, a^{14} - 1) = (a^7 - 1, a^{14} - 1) = (a^{14} - 1, a^7 - 1) \\ &= (a^7 - 1, a^7 - 1) = a^7 - 1. \end{aligned}$$

In abbreviated form, this would read

$$(a^{84} - 1, a^{35} - 1) = (a^{35} - 1, a^{14} - 1) = (a^{14} - 1, a^7 - 1) = (a^7 - 1, 0) = a^7 - 1,$$

which we contrast with $(84, 35) = (35, 14) = (14, 7) = (7, 0) = 7$.

Theorem. If $d \mid 2^p - 1$, then $d \equiv 1 \pmod{p}$.

Proof. Let $q \mid 2^p - 1$, where q is prime. By Little Fermat, $2^{q-1} \equiv 1 \pmod{q}$. This means that $q \mid 2^{q-1} - 1$ and $q \mid 2^p - 1$. Consequently, q is a common divisor of these two numbers, so $q \mid (2^{q-1} - 1, 2^p - 1)$. By the previous lemma, $(2^{q-1} - 1, 2^p - 1) = 2^{(q-1, p)} - 1$. If $(p, q-1) = 1$, then we have that $q \mid 2^1 - 1 = 1$, which can't be. Thus, $(p, q-1) > 1$. But the greatest common divisor of a prime with anything is either 1 or the prime, so $(p, q-1) = p$. This means that p must be a divisor of $q-1$, which says that $q \equiv 1 \pmod{p}$. Finally, if d is any divisor of $2^p - 1$, then d can be factored into primes $d = q_1 q_2 \cdots q_k$ and each q is congruent to 1 modulo p . Thus the product, d , will also be congruent to 1 modulo p .

Fast Exponentiation

In order to apply Fermat's little theorem as a compositeness test, we must have a reasonable way to calculate $a^n \pmod{n}$ relatively quickly. There is such a method. It is based on the following fact: $a^{2^n} = (a^{2^{n-1}})^2$. We will show the method with an example. Suppose we wish to verify that 341 is not a base 3 pseudoprime. That is, we wish to calculate $3^{340} \pmod{341}$. We use the following method:

Step 1: Write 340 as a sum of powers of 2: $340 = 256 + 64 + 16 + 4$. From this, it follows that $3^{340} = 3^{256+64+16+4} = 3^{256} 3^{64} 3^{16} 3^4$

Step 2: Construct a table of terms $3^{2^n} \pmod{341}$ by repeatedly squaring results:

n	0	1	2	3	4	5	6	7	8
2^n	1	2	4	8	16	32	64	128	256
$3^{2^n} \pmod{341}$	3	9	81	82	245	9	81	82	245

Step 3: Put the results of steps 1 and 2 together: $3^{340} \equiv 245 \cdot 9 \cdot 245 \cdot 81 \equiv 56 \pmod{341}$

This is called the **Binary Squaring** method.

Both Maple and Mathematica know about the binary squaring method. To calculate $a^k \pmod{n}$ in these packages, you can do this:

Maple

$a \&^k \pmod{n}$;

Mathematica

PowerMod[a, k, n]