THE ORDER MODULO m

Let m be a positive integer.

Lemma 0.1. *For any integer a such that $(a, m) = 1$ there exists $k >$ such that $0 < k < m$ and $a^k \equiv 1 \pmod{m}$.*

Proof. Consider the numbers $a, a^2, \ldots, a^m$. Since there are only $m - 1$ possible non-zero remainders upon division by m, two of these m numbers must give the same remainder, i.e. for some $1 \leq s < t \leq m$ we must have $a^t \equiv a^s \pmod{m}$. Since $(a^s, m) = 1$, we can divide the last congruence by a^s and get $a^{t-s} \equiv 1 \pmod{m}$. Thus $k = t - s$ works. □

Remark 0.2. The existence of such k follows immediately from Euler's Theorem, but the proof above is simpler than a proof of Euler's Theorem.

Lemma 0.1 allows us to make the following definition. For any integer a such that $(a, m) = 1$ we define the **order of a modulo m** as the smallest positive integer k such that $a^k \equiv 1 \pmod{m}$. We denote it by $\mathrm{ord}_m a$. Thus

$$a^{\mathrm{ord}_m a} \equiv 1 \pmod{m}$$

and

$$a^t \not\equiv 1 \pmod{m}$$

for any t such that $0 < t < \mathrm{ord}_m a$.

The function ord_m has the following fundamental properties:

Property 1. The congruence $a^k \equiv 1 \pmod{m}$ holds if and only if $\mathrm{ord}_m a | k$.

Proof. According to the division algorithm, we can write $k = n \cdot \mathrm{ord}_m a + r$, where $0 \leq r < \mathrm{ord}_m a$. Thus

$$a^k = (a^{\mathrm{ord}_m a})^n a^r \equiv 1^n \cdot a^r = a^r \pmod{m} .$$

It follow that $a^k \equiv 1 \pmod{m}$ if and only if $a^r \equiv 1 \pmod{m}$. But since $r < \mathrm{ord}_m a$, the last congruence holds if and only if $r = 0$. Thus we showed that $a^k \equiv 1 \pmod{m}$ iff $r = 0$, i,e, if and only if $\mathrm{ord}_m a | k$. □

Property 2. If $(a, m) = 1$ then $a^s \equiv a^t \pmod{m}$ if and only if $\mathrm{ord}_m a | (s - t)$.

Proof. We may assume that $t \leq s$. Since $(a^t, m) = 1$, the congruence $a^s \equiv a^t \pmod{m}$ is equivalent to $a^{s-t} \equiv 1 \pmod{m}$ (cancelling a^t). By Property 1, the last congruence holds iff $\mathrm{ord}_m a | (s - t)$. □

Corollary 0.3. *No two of the numbers $1, a, a^2, \ldots, a^{\mathrm{ord}_m a - 1}$ are congruent to each other modulo m.*

Property 3.

$$\mathrm{ord}_m a^n = \frac{\mathrm{ord}_m a}{(n, \mathrm{ord}_m a)}$$

for all natural numbers n and any a relatively prime to m.

Proof. By Property 1, $(a^n)^k = a^{nk} \equiv 1 \pmod m$ if and only if $\mathrm{ord}_m a | nk$. The last divisibility is equivalent to $\frac{\mathrm{ord}_m a}{(n,\mathrm{ord}_m a)} \Big| \frac{n}{(n,\mathrm{ord}_m a)} k$. Since the numbers $\frac{\mathrm{ord}_m a}{(n,\mathrm{ord}_m a)}$ and $\frac{n}{(n,\mathrm{ord}_m a)}$ are relatively prime, the last divisibility is in turn equivalent to $\frac{\mathrm{ord}_m a}{(n,\mathrm{ord}_m a)} \Big| k$. Thus we proved that $(a^n)^k \equiv 1 \pmod m$ if and only if $\frac{\mathrm{ord}_m a}{(n,\mathrm{ord}_m a)} \Big| k$. This clearly implies that $\mathrm{ord}_m a^n = \frac{\mathrm{ord}_m a}{(n,\mathrm{ord}_m a)}$. □

The next property will relate $\mathrm{ord}_m(ab)$ to $\mathrm{ord}_m a$ and $\mathrm{ord}_m b$.

Property 4. Let a, b be integers both relatively prime to m. Then

(i) $\mathrm{ord}_m(ab) \Big| \dfrac{\mathrm{ord}_m a \cdot \mathrm{ord}_m b}{(\mathrm{ord}_m a, \mathrm{ord}_m b)}$.

(ii) $\dfrac{\mathrm{ord}_m a \cdot \mathrm{ord}_m b}{(\mathrm{ord}_m a, \mathrm{ord}_m b)^2} \Big| \mathrm{ord}_m(ab)$.

Proof. To make the notation simpler, set $u = \mathrm{ord}_m a, w = \mathrm{ord}_m b$. Note that $\frac{uw}{(u,w)} = u\frac{w}{(u,w)} = w\frac{u}{(u,w)}$, so the number $\frac{uw}{(u,w)}$ is divisible by both u and w. It follows by Property 1 that $a^{\frac{uw}{(u,w)}} \equiv 1 \pmod m$ and $a^{\frac{uw}{(u,w)}} \equiv 1 \pmod m$. Multiplying these congruences, we get $(ab)^{\frac{uw}{(u,w)}} \equiv 1 \pmod m$. Thus, by Property 1 again, we have $\mathrm{ord}_m(ab) | \frac{uw}{(u,w)}$. This proves (i).

By Property 1, we have $a^{u \cdot \mathrm{ord}_m(ab)} \equiv 1 \pmod m$. Multiply both sides by $b^{u \cdot \mathrm{ord}_m(ab)}$ to get $(ab)^{u \cdot \mathrm{ord}_m(ab)} \equiv b^{u \cdot \mathrm{ord}_m(ab)} \pmod m$. But $(ab)^{u \cdot \mathrm{ord}_m(ab)} \equiv 1 \pmod m$ (by Property 1). Thus $b^{u \cdot \mathrm{ord}_m(ab)} \equiv 1 \pmod m$. By Property 1 once again, we have $w | u \cdot \mathrm{ord}_m(ab)$. This means that $\frac{w}{(u,w)} \Big| \frac{u}{(u,w)} \cdot \mathrm{ord}_m(ab)$. Since the numbers $\frac{w}{(u,w)}$ and $\frac{u}{(u,w)}$ are relatively prime, we conclude that $\frac{w}{(u,w)} \Big| \mathrm{ord}_m(ab)$.

In exactly the same way, changing the roles of a and b, we prove that $\frac{u}{(u,w)} \Big| \mathrm{ord}_m(ab)$. Thus both $\frac{w}{(u,w)}$ and $\frac{u}{(u,w)}$ divide $\mathrm{ord}_m(ab)$ and since these numbers are relatively prime, their product also divides $\mathrm{ord}_m(ab)$, i.e. $\frac{uw}{(u,w)^2} \Big| \mathrm{ord}_m(ab)$. This proves (ii). □

Note that the right hand side in (i) is equal to the least common multiple of $\mathrm{ord}_m a$ and $\mathrm{ord}_m b$. Property 4 allows to locate ord_{ab} within the numbers $\frac{\mathrm{ord}_m a \cdot \mathrm{ord}_m b}{(\mathrm{ord}_m a, \mathrm{ord}_m b)^2}$ and $\frac{\mathrm{ord}_m a \cdot \mathrm{ord}_m b}{(\mathrm{ord}_m a, \mathrm{ord}_m b)}$. Note that in general one can not say much more. For example, if $\mathrm{ord}_5 2 = 4 = \mathrm{ord}_5 3$ and $\mathrm{ord}_5(2 \cdot 3) = 1$. On the other hand, $\mathrm{ord}_5(2 \cdot 2) = 2$. When $(\mathrm{ord}_m a, \mathrm{ord}_m b) = 1$ however both upper and lower bounds are the same so as a corollary we get the following property.

Property 5. Let a, b be integers both relatively prime to m. If $(\mathrm{ord}_m a, \mathrm{ord}_m b) = 1$ then

$$\mathrm{ord}_m(ab) = \mathrm{ord}_m a \cdot \mathrm{ord}_m b.$$

Exercise. Write a direct proof of Property 5 simplifying the arguments in the proof of Property 4.

We can now prove the following very useful result.

Theorem 0.4. *Let a be an integer relatively prime to m whose order modulo m is largest possible. Then $\mathrm{ord}_m b | \mathrm{ord}_m a$ for every integer b.*

Proof. Let p be a prime. We may write $\mathrm{ord}_m a = p^s u$, $\mathrm{ord}_m b = p^t w$ for some non-negative s, t and some integers u, w not divisible by p. By Property 3, $\mathrm{ord}_m a^{p^s} = u$ and $\mathrm{ord}_m b^w = p^t$. Since $(u, p^t) = 1$, Property 5 tells us that $\mathrm{ord}_m(a^{p^s} b^w) = p^t u$. Since $p^s u$ is the largest possible order modulo m, we have $p^t u \leq p^s u$, i.e. $t \leq s$. This shows that every prime which contributes to $\mathrm{ord}_m b$ contributes at lest the same to $\mathrm{ord}_m a$. Thus $\mathrm{ord}_m b | \mathrm{ord}_m a$. □

Definition 0.5. *The largest possible exponent of an integer modulo m is denoted by $\lambda(m)$. It is often called the* **smallest universal exponent modulo** *m, since by Theorem 0.4 it is the smallest exponent $k > 0$ such that $b^k \equiv 1 \pmod{m}$ holds for every b relatively prime to m.*

Our goal is to compute $\lambda(p)$ for prime numbers p. Note that the congruence $x^{\lambda(p)} \equiv 1 \pmod{p}$ is satisfied by every integer not divisible by p, i.e. it has $p-1$ different solutions modulo p. We will prove the following important theorem.

Theorem 0.6 (Lagrange)**.** *Let p be a prime and let $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ be a polynomial with integral coefficients not all of which are divisible by p. Then the congruence $f(x) \equiv 0 \pmod{p}$ has at most n different modulo p solutions.*

Proof. We proceed by induction on the degree n. When the degree is 0 then $f = a_0$ is a constant which is not divisible by p, hence the congruence has no solutions. Suppose that the result holds for all polynomials of degree less than n (which satisfy the assumptions of the theorem) and consider a polynomial $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ with at least one coefficient not divisible by p. If the congruence $f(x) \equiv 0 \pmod{p}$ has no solutions, the result clearly holds for f. Suppose then that there is a solution u to this congruence. Recall now the following identity for any positive integer k:

$$x^k - u^k = (x-u)(x^{k-1} + x^{k-2}u + \ldots + xu^{k-2} + u^{k-1}).$$

It follows that we have

$$f(x) - f(u) = a_1(x-u) + a_2(x^2 - u^2) + \ldots + a_n(x^n - u^n) = (x-u)h(x)$$

for some polynomial $h(x)$ with integral coefficients and of degree less than n. If all coefficients of h were divisible by p, the same would hold for f, since $p | f(u)$. Suppose now that w is another solution to $f(x) \equiv 0 \pmod{p}$, which is different from u modulo p. Then $p | f(w) - f(u) = (w-u)h(w)$. Since $p \nmid (w-u)$, we have $p | h(w)$. In other words, w is a solution to $h(x) \equiv 0 \pmod{p}$. By the inductive assumption, there are at most $n-1$ different modulo p such w's. Thus $f(x) \equiv 0 \pmod{p}$ has indeed at most n different solutions modulo p. The result holds then by induction. □

As an immediate corollary we see that the congruence $x^{\lambda(p)} \equiv 1 \pmod{p}$ has at most $\lambda(p)$ solutions. On the other hand, we know that it has $p-1$ solutions, so $\lambda(p) \geq p-1$. On the other hand, Lemma 0.1 implies that $\lambda(p) \leq p-1$ (since $\lambda(p)$ is the order of some integer). Thus $\lambda(p) = p-1$. Thus we get the following two important results.

Theorem 0.7 (Fermat's Little Theorem)**.** *Let p be a prime. If a is an integer and $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$.*

Theorem 0.8. *Let p be a prime. There exists an integer a such that $\mathrm{ord}_p a = p-1$.*

Any integer a as in the last theorem is called a **primitive root modulo** p.

Lagrange's Theorem (Theorem 0.6) has many important applications. For example, consider the polynomial $F(x) = x^{p-1} - 1 - (x-1)(x-2)\dots(x-(p-1))$. It is easy to see that the degree of this polynomial is less than $p-1$ (x^{p-1} cancels out). However, by Fermat's Little Theorem, every integer prime to p satisfies the congruence $F(x) \equiv 0 \pmod{p}$, i.e. this congruence has $p-1$ different solutions modulo p. By Lagrange's Theorem, all coefficients of F must be divisible by p. In particular, the constant term $-1-(-1)(-2)\dots(-(p-1))$ is divisible by p. Thus we get the following theorem.

Theorem 0.9 (Wilson)**.** *For every prime p we have $(p-1)! \equiv -1 \pmod{p}$.*

It is easy to see that the converse is also true. More precisely, if n is not a prime then $(n-1)! \equiv 0 \pmod{n}$.

Exercise. Look at other coefficients of F and derive some congruences.

Suppose now that g is a primitive root modulo a prime p. By Property 2, the numbers $1, g, g^2, ..., g^{p-2}$ are all distinct modulo p. It follows that Thus these numbers form a complete set each number relatively prime to p is congruent to exactly one of these numbers. Recall that by Property 3, the order of g^k modulo p is $\dfrac{p-1}{(k,p-1)}$. We ask: how many of these numbers have a given order d? This only makes sense for $d|p-1$. Given such d we want to count all k such that $1 \le k < p-1$ and $(k,p-1) = \frac{p-1}{d}$. In other words, $k = \frac{p-1}{d}k_1$ and $(k_1, d) = 1$. Moreover $1 \le k_1 < d$. There are exactly $\phi(d)$ such k. Thus we have the following result.

Theorem 0.10. *Let p be a prime and let $d|p-1$. Among the non-zero residues modulo p there are exactly $\phi(d)$ which have order d modulo p. In particular, there are exactly $\phi(p-1)$ different primitive roots modulo p. They are g^k, where $1 \le k < p-1$ and $(k, p-1) = 1$.*

The distribution of primitive roots has been the subject of many investigations. One of the outstanding open problems about primitive roots is the following Conjecture.

Conjecture 0.11 (Artin)**.** *Let $a \ne -1$ be an ineteger which is not a square. Then there are infinitely many primes p for which a is a primitive root modulo p.*

In fact, this is not known for even a single value of a. On the other hand, it is know that the conjecture follows from so called Generalized Riemann Hypothesis, which is one of the most important conjectures in number theory. It is know that there are at most two prime numbers a for which Artin's conjecture could fail. Thus, we can prove that Artin's conjecture is true for one of the numbers 2,3,5 but we do not know for which.