

14. Euler's Theorem.

This is a generalization of Fermat's Theorem to the case of *composite* modulus.

Lemma Suppose that $m \in \mathbf{N}$ and $k \in \mathbf{Z}$ with $\gcd(m,k) = 1$.
If $R = \{r(1), \dots, r(\varphi(m))\}$ is an RSR (mod m), then so is $kR = \{kr(1), \dots, kr(\varphi(m))\}$.

Note. This is similar to the Lemma in Chapter 13. The proof follows similar lines.

Proof

Suppose that the given R is an RSR modulo m . This means that the $r(i)$ are

- (1) distinct modulo m , and
- (2) coprime with m .

Conversely, a set of $\varphi(m)$ integers satisfying (1) and (2) is an RSR modulo m .

As in the proof of the Lemma in Chapter 13, the $kr(i)$ are distinct modulo m .
Thus, kR satisfies condition (1).

We are also given that $\gcd(k,m) = 1$, and that R satisfies condition (2), i.e. $\gcd(r(i),m) = 1$.
Thus, kR satisfies condition (2).

Hence kR is an RSR modulo m .

Theorem 1. Euler's Theorem.

If $m \in \mathbf{N}$ and $a \in \mathbf{Z}$ with $\gcd(a,m) = 1$, then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Proof

Let $R = \{r(1), \dots, r(\varphi(m))\}$ be an RSR modulo m .

As $\gcd(a,m) = 1$, the Lemma shows that aR is also an RSR modulo m .

Thus, the members of aR are congruent modulo m to those of R in some order.

Taking the products of each set, we get

$$ar(1) \dots ar(\varphi(m)) \equiv r(1) \dots r(\varphi(m)) \pmod{m}$$

As each $r(i)$ is coprime to m , we can cancel it from each side. We are left with

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

Example Show that, if $\gcd(a,561) = 1$, then $a^{320} \equiv 1 \pmod{561}$.

Solution

As $561 = 3 \cdot 11 \cdot 17$, $\varphi(561) = \varphi(3)\varphi(11)\varphi(17) = 2 \cdot 10 \cdot 16 = 320$.

Now $\gcd(a,561) = 1$, so Euler's Theorem tell us that $a^{320} \equiv 1 \pmod{561}$.

Example continued.

An example in Chapter 13, shows that, for any a , $a^{561} \equiv a \pmod{561}$.

Deduce from that and the previous example that, if $\gcd(a, 561) = 1$, then $a^{80} \equiv 1 \pmod{561}$.

Solution.

The previous example shows that $a^{320} \equiv 1 \pmod{561}$.

Squaring each side, we get $a^{640} = (a^{320})^2 \equiv 1^2 \equiv 1 \pmod{561}$.

From the example in Chapter 13, $a^{561} \equiv a \pmod{561}$.

Here, we are given that $\gcd(a, 561) = 1$, so we can cancel a from each side to get the new congruence $a^{560} \equiv 1 \pmod{561}$.

Then $1 \equiv a^{640} \equiv a^{560} a^{80} \equiv 1 \cdot a^{80} \equiv a^{80} \pmod{561}$, as required.

Note

For integer b greater than 1, the last d “digits” when N is written in base b is the remainder when N is divided by b^d , i.e. it is the integer r such that $N \equiv r \pmod{b}$, and $0 \leq r < b^d$.

Example Find the last three digits when 2007^{2007} is written in decimal notation.

Solution

Observe that the last three digits of the integer N written in base 10 gives the remainder when N is divided by 1000. Thus, here we need to compute the remainder, r , when N is divided by 1000.

Since $2007 \equiv 7 \pmod{1000}$, $2007^{2007} \equiv 7^{2007} \equiv (7) \pmod{1000}$

Now $1000 = 2^3 \cdot 5^3$, so $\phi(1000) = 2^{3-1} \cdot 2 \cdot 5^{3-1} \cdot 4 = 400$, and $\gcd(7, 1000) = 1$, so that Euler’s Theorem gives

$$7^{2007} = (7^{400})^5 \cdot 7^7 \equiv 1^5 \cdot 7^7 \equiv 7^7 \pmod{1000}.$$

By direct calculation, $7^7 = 823543 \equiv 543 \pmod{1000}$.

Thus, the last three digits are “543”.

Exercise to reader Show that $\phi(10^k) = 4 \cdot 10^k$.

The order of a modulo m .

Suppose that $m \in \mathbf{N}$ and $a \in \mathbf{Z}$ with $\gcd(a, m) = 1$. By Euler’s Theorem $a^{\phi(m)} \equiv 1 \pmod{m}$. Of course, there may be other $k \in \mathbf{N}$ with $a^k \equiv 1 \pmod{m}$.

Definition Suppose that $m \in \mathbf{N}$ and $a \in \mathbf{Z}$ with $\gcd(a, m) = 1$. The *order of a modulo m* is the least positive integer k with $ak \equiv 1 \pmod{m}$. This is denoted by $\text{ord}_m(a)$.

After the above remark, the order of a modulo m is *always* defined, and can never be greater than $\phi(m)$. Also, $a^1 \equiv 1 \pmod{m}$ if and only if $a \equiv 1 \pmod{m}$, so if a is *not* congruent to 1 modulo m , then the order of a modulo m is *greater* than 1.

Example Find the order of 3 modulo 5.

Solution

$3^2 = 9 \equiv 4 \pmod{5}$, so $3^3 = 3 \cdot 3^2 \equiv 3 \cdot 4 \equiv 2 \pmod{5}$, Then $3^4 = 3 \cdot 3^3 \equiv 3 \cdot 2 \equiv 1 \pmod{5}$. Thus, 4 is the *least* positive integer k with $3^k \equiv 1 \pmod{5}$, i.e. $\text{ord}_5(3) = 4$.

Exercise to reader Find $\text{ord}_5(4)$.

Observe that $\varphi(5) = 4$. The example gives a case of an element a with $\text{ord}_m(a) = \varphi(m)$. Your answer to the exercise should be 2, an example with $\text{ord}_m(a) < \varphi(m)$.

Theorem 2

Suppose that $m \in \mathbf{N}$ and $a \in \mathbf{Z}$ with $\text{gcd}(a, m) = 1$. Then, for $h \in \mathbf{N}$, $a^h \equiv 1 \pmod{m} \Leftrightarrow \text{ord}_m(a) \mid h$.

Proof

Let $k = \text{ord}_m(a)$. Then

- (1) $a^k \equiv 1 \pmod{m}$, and
- (2) if $a^K \equiv 1 \pmod{m}$ and $K > 0$, then $K \geq k$ (since k is *least*).

We are given that $a^h \equiv 1 \pmod{m}$ and $h \in \mathbf{N}$, so that $h > 0$. By the Division Theorem, $h = qk + r$, with $q \in \mathbf{N}$ and $0 \leq r < k$.

$$\begin{aligned} \text{Then} \quad 1 &\equiv a^h \pmod{m} \\ &\equiv (a^k)^q \cdot a^r \pmod{m}, \quad \text{as } h = kq+r \\ &\equiv 1^q \cdot a^r \equiv a^r \pmod{m}, \quad \text{as } a^k \equiv 1 \pmod{m} \end{aligned}$$

Thus, $a^r \equiv 1 \pmod{m}$, so (2) gives $r \geq k$ if $r > 0$. But $0 \leq r < k$ from the Division Theorem. The only way these can happen together is if we have $r = 0$.

Then $h = kq + r = kq$, as $r = 0$. Thus we have $k \mid h$.

Corollary Provided $\text{gcd}(a, m) = 1$, $\text{ord}_m(a) \mid \varphi(m)$.

Proof By Euler's Theorem, $a^{\varphi(m)} \equiv 1 \pmod{m}$. Then, by Theorem 2, $\text{ord}_m(a) \mid \varphi(m)$.

Exercise Find the orders of 1, 2, 3, 4, 5, 6 modulo 7.

Solution

As $\varphi(7) = 6$, by the Corollary, $\text{ord}_7(a) \mid 6$, so $\text{ord}_7(a)$ can only be 1, 2, 3 or 6. Thus, if we check that the order is *not* 1, 2 or 3, then it *must* be 6. This helps with $a = 3, 5$ below.

$$\begin{aligned} 1^1 &= 1, \text{ so } \text{ord}_7(1) = 1 \text{ (ord}_m(1) \text{ is always 1).} \\ 2^1 &= 2, 2^2 = 4, 2^3 = 8 \equiv 1 \pmod{7}, \text{ so } \text{ord}_7(2) = 3, \\ 3^1 &= 3, 3^2 = 9 \equiv 2 \pmod{7}, 3^3 \equiv 3 \cdot 2 \equiv 6 \pmod{7}, \text{ so } \text{ord}_7(3) = 6, \\ 4^1 &= 4, 4^2 = 16 \equiv 2 \pmod{7}, 4^3 \equiv 4 \cdot 2 \equiv 1 \pmod{7}, \text{ so } \text{ord}_7(4) = 3, \\ 5^1 &= 5, 5^2 = 25 \equiv 4 \pmod{7}, 5^3 \equiv 5 \cdot 4 \equiv 6 \pmod{7}, \text{ so } \text{ord}_7(5) = 6, \\ 6^1 &= 6, 6^2 = 36 \equiv 1 \pmod{7}, \text{ so } \text{ord}_7(6) = 2. \end{aligned}$$

Example Suppose that $a, m \in \mathbf{N}$, with $\gcd(a, m) = 1$. Let $k = \text{ord}_m(a)$. Show that the integers a, a^2, a^3, \dots, a^k are distinct modulo m .

Solution

Suppose not.

Then there must be integers i, j with $1 \leq i < j \leq k$ and $a^i \equiv a^j \pmod{m}$.

As $\gcd(a, m) = 1$, we can cancel a^i from each side to get $a^{j-i} \equiv 1 \pmod{m}$.

As $1 \leq i < j \leq k$, $0 < j-i < k$.

From Theorem 2, and the facts that $a^{j-i} \equiv 1 \pmod{m}$ and $0 < j-i$, we get $k \leq j-i$

This contradicts the inequality $j-i < k$ in the previous line.

Hence, the result must be true.

Example Suppose that $a, k, m \in \mathbf{N}$, with $\gcd(a, m) = \gcd(k, \text{ord}_m(a)) = 1$. Show that

$$\text{ord}_m(a^k) = \text{ord}_m(a).$$

Solution

Let $A = \text{ord}_m(a)$, so $a^A \equiv 1 \pmod{m}$, and A is the least positive integer with this property.

Then

$$(a^k)^A = (a^A)^k \equiv 1^k \equiv 1 \pmod{m}.$$

Thus $\text{ord}_m(a^k)$ is *at most* A , as this power of a is already 1.

Now suppose that $C > 0$ is such that $(a^k)^C \equiv 1 \pmod{m}$.

Then $a^{kC} \equiv 1 \pmod{m}$, so that $A \mid kC$, by Theorem 2.

Now $\gcd(k, A) = 1$, so Euclid's Lemma gives $A \mid C$.

Thus, $\text{ord}_m(a^k)$ is *at least* A , from the definition of order.

Hence, $\text{ord}_m(a^k) = A = \text{ord}_m(a)$.

Note. The condition $\gcd(k, \text{ord}_m(a)) = 1$ in the previous example is *necessary*.

If $m = 15$, and $a = 2$, the powers of 2 are $2, 2^2 = 4, 2^3 = 8, 2^4 = 16 \equiv 1 \pmod{15}$.

Thus, $\text{ord}_{15}(2) = 4$, the least positive power of 2 congruent to 1 modulo 15.

Now we note that $4 = 2^2$ has $4^2 = 16 \equiv 1 \pmod{15}$, so $\text{ord}_{15}(4) = 2$.

This is an example where $\text{ord}_{15}(4) = \text{ord}_{15}(2^2) \neq \text{ord}_{15}(2)$.

Exercise to reader. Verify that $\text{ord}_{15}(2^3) = 4$, in line with the previous example.

Theorem 3 The integer a is a solution of $x^n \equiv 1 \pmod{m} \Leftrightarrow \text{ord}_m(a) \mid n$.

Proof

If $\text{ord}_m(a) \mid n$, then $a^n \equiv 1 \pmod{m}$, by Theorem 2.

Now suppose that $a^n \equiv 1 \pmod{m}$. Then $\text{ord}_m(a) \mid n$, again by Theorem 2.

Note that $a = 1$ is *always* a solution of $x^n \equiv 1 \pmod{m}$.

This fits with Theorem 3 since $\text{ord}_m(a) = 1$.

In the real numbers, the equation $x^2 = 1$ has *exactly two* solutions, $x = \pm 1$.

For the congruence version, $x^2 \equiv 1 \pmod{m}$, things may be different.

Example.

(1) If p is an odd prime, then $x^2 \equiv 1 \pmod{p}$ has exactly two solutions, $x \equiv \pm 1 \pmod{p}$.

(2) If $m = pq$, with p and q *distinct odd primes*, then $x^2 \equiv 1 \pmod{m}$ has *four* solutions.

Solution.

(1) $x^2 \equiv 1 \pmod{p} \Leftrightarrow x^2 - 1 = (x-1)(x+1) \equiv 0 \pmod{p}$.

Thus, $p \mid (x-1)(x+1)$.

As p is prime, $p \mid (x-1)$ so $x \equiv 1 \pmod{p}$, or $p \mid (x+1)$, so $x \equiv -1 \pmod{p}$.

Thus, we have *precisely* the two solutions indicated.

(2) Suppose that $x^2 \equiv 1 \pmod{m = pq}$.

Then $x^2 \equiv 1 \pmod{p}$, so $x \equiv \pm 1 \pmod{p}$, by part (1).

Likewise, $x^2 \equiv 1 \pmod{q}$, so $x \equiv \pm 1 \pmod{q}$.

Thus, we have *four* types of solution :

$x \equiv 1 \pmod{p}$, $x \equiv 1 \pmod{q}$: this gives $x \equiv 1 \pmod{m}$,

$x \equiv 1 \pmod{p}$, $x \equiv -1 \pmod{q}$,

$x \equiv -1 \pmod{p}$, $x \equiv 1 \pmod{q}$,

$x \equiv -1 \pmod{p}$, $x \equiv -1 \pmod{q}$: this gives $x \equiv -1 \pmod{m}$.

By the Chinese Remainder Theorem, each type gives a *congruence class* modulo m .

We will meet this result again in the final Chapter.

Illustration If we take $m = 15$, so $p = 3$, $q = 5$, and part (2) applies. The reader may verify that the solutions are $x \equiv 1$ or 4 or 11 or $14 \pmod{15}$.