Introduction to number theory-6

May 1, 2017

Theorem 2.2 *Let m, a, b be integers with $m \geq 1$. Let $d = (a, m)$ be the greatest common divisor of a and m. The congruence*

$$ax \equiv b \pmod{m} \tag{2.1}$$

has a solution if and only if

$$b \equiv 0 \pmod{d}.$$

If $b \equiv 0 \pmod{d}$, then the congruence (2.1) has exactly d solutions in integers that are pairwise incongruent modulo m. In particular, if $(a, m) = 1$, then for every integer b the congruence (2.1) has a unique solution modulo m.

Proof. Let $d = (a, m)$. Congruence (2.1) has a solution if and only if there exist integers x and y such that

$$ax - b = my,$$

or, equivalently,

$$b = ax - my.$$

By this is possible if and only if $b \equiv 0 \pmod{d}$.

If x and x_1 are solutions of (2.1), then

$$a(x_1 - x) \equiv ax_1 - ax \equiv b - b \equiv 0 \pmod{m},$$

and so

$$a(x_1 - x) = mz$$

for some integer z. If d is the greatest common divisor of a and m, then $(a/d, m/d) = 1$ and

$$\left(\frac{a}{d}\right)(x - x_1) = \left(\frac{m}{d}\right) z.$$

By Euclid's lemma (Theorem 1.7), m/d divides $x_1 - x$, and so

$$x_1 = x + \frac{im}{d}$$

for some integer i, that is,

$$x_1 \equiv x \pmod{\frac{m}{d}}.$$

Moreover, every integer x_1 of this form is a solution of (2.1). An integer x_1 congruent to x modulo m/d is congruent to $x + im/d$ modulo m for some integer $i = 0, 1, \ldots d-1$, and the d integers $x+im/d$ with $i = 0, 1, \ldots, d-1$ are pairwise incongruent modulo m. Thus, the congruence (2.1) has exactly d pairwise incongruent solutions. This completes the proof. □

Theorem 2.3 *If p is a prime, then $\mathbf{Z}/p\mathbf{Z}$ is a field.*

Proof. If $a + p\mathbf{Z} \in \mathbf{Z}/p\mathbf{Z}$ and $a + p\mathbf{Z} \neq p\mathbf{Z}$, then a is an integer not divisible by p. By Theorem 2.2, there exists an integer x such that $ax \equiv 1 \pmod{p}$. This implies that

$$(a + p\mathbf{Z})(x + p\mathbf{Z}) = 1 + p\mathbf{Z},$$

and so $a + p\mathbf{Z}$ is invertible. Thus, every nonzero congruence class in $\mathbf{Z}/p\mathbf{Z}$ is a unit and $\mathbf{Z}/p\mathbf{Z}$ is a field. □

Here are some examples of linear congruences. The congruence

$$7x \equiv 3 \pmod 5$$

has a unique solution modulo 5 since $(7, 5) = 1$. The solution is $x \equiv 4 \pmod 5$. The congruence

$$35x \equiv -14 \pmod{91} \tag{2.2}$$

is solvable since $(35, 91) = 7$ and

$$-14 \equiv 0 \pmod 7.$$

Congruence (2.2) is equivalent to the congruence

$$5x \equiv -2 \pmod{13}, \tag{2.3}$$

which has the unique solution $x \equiv 10 \pmod{13}$. Every solution of (2.2) satisfies

$$x \equiv 10 \pmod{13}$$

and so a complete set of solutions that are pairwise incongruent modulo 91 is $\{10, 23, 36, 49, 62, 75, 88\}$.

Lemma 2.1 *Let p be a prime number. Then $x^2 \equiv 1 \pmod{p}$ if and only if $x \equiv \pm 1 \pmod{p}$.*

Proof. If $x \equiv \pm 1 \pmod{p}$, then $x^2 \equiv 1 \pmod{p}$. Conversely, if $x^2 \equiv 1 \pmod{p}$, then p divides $x^2 - 1 = (x-1)(x+1)$, and so p must divide $x-1$ or $x+1$. $\square$

Theorem 2.4 (Wilson) *If p is prime, then*

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. This is true for $p = 2$ and $p = 3$, since $1! \equiv -1 \pmod{2}$ and $2! \equiv -1 \pmod{3}$. Let $p \geq 5$. By Theorem 2.2, to each integer $a \in \{1, 2, \ldots, p-1\}$ there is a unique integer $a^{-1} \in \{1, 2, \ldots, p-1\}$ such that $aa^{-1} \equiv 1 \pmod{p}$. By Lemma 2.1, $a = a^{-1}$ if and only if $a = 1$ or $a = p-1$. Therefore, we can partition the $p-3$ numbers in the set $\{2, 3, \ldots, p-2\}$ into $(p-3)/2$ pairs of integers $\{a_i, a_i^{-1}\}$ such that $a_i a_i^{-1} \equiv 1 \pmod{p}$ for $i = 1, \ldots, (p-3)/2$. Then

$$\begin{aligned}
(p-1)! &\equiv 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1) \\
&\equiv (p-1) \prod_{i=1}^{(p-3)/2} a_i a_i^{-1} \\
&\equiv p-1 \\
&\equiv -1 \pmod{p}.
\end{aligned}$$

This completes the proof. □

Prove that if m is composite and $m \neq 4$, then $(m-1)! \equiv 0 \pmod{m}$.
This is the converse of Wilson's theorem.

Theorem 2.5 *Let m and d be positive integers such that d divides m. If a is an integer relatively prime to d, then there exists an integer a' such that $a' \equiv a \pmod{d}$ and a' is relatively prime to m.*

Proof. Let $m = \prod_{i=1}^{k} p_i^{r_i}$ and $d = \prod_{i=1}^{k} p_i^{s_i}$, where $r_i \geq 1$ and $0 \leq s_i \leq r_i$ for $i = 1, \ldots, k$. Let m' be the product of the prime powers that divide m but not d. Then

$$m' = \prod_{\substack{i=1 \\ s_i=0}}^{k} p_i^{r_i}$$

and

$$(m', d) = 1.$$

By Theorem 2.2, there exists an integer x such that

$$dx \equiv 1 - a \pmod{m'}.$$

Then

$$a' = a + dx \equiv 1 \pmod{m'}$$

and so

$$(a', m') = 1.$$

Also,

$$a' \equiv a \pmod{d}.$$

If $(a', m) \neq 1$, there exists a prime p that divides both a' and m. However, p does not divide m' since $(a', m') = 1$. It follows that p divides d, and so p divides $a' - dx = a$, which is impossible since $(a, d) = 1$. Therefore, $(a', m) = 1$. □

If $a \equiv b \pmod{m}$, then $a = b + mx$ for some integer x. An integer d is a common divisor of a and m if and only if d is a common divisor of b and m, and so $(a, m) = (b, m)$. In particular, if a is relatively prime to m, then every integer in the congruence class of $a + m\mathbf{Z}$ is relatively prime to m. A congruence class modulo m is called *relatively prime to* m if some (and, consequently, every) integer in the class is relatively prime to m.

We denote by $\varphi(m)$ the number of congruence classes in $\mathbf{Z}/m\mathbf{Z}$ that are relatively prime to m. The function $\varphi(m)$ is called the *Euler phi function*. Equivalently, $\varphi(m)$ is the number of integers in the set $0, 1, 2, \ldots, m-1$ that are relatively prime to m. The Euler phi function is also called the *totient function*.

A set of integers $\{r_1, \ldots, r_{\varphi(m)}\}$ is called a *reduced set of residues* modulo m if every integer x such that $(x, m) = 1$ is congruent modulo m to some integer r_i. For example, the sets $\{1, 2, 3, 4, 5, 6\}$ and $\{2, 4, 6, 8, 10, 12\}$ are reduced sets of residues modulo 7. The sets $\{1, 3, 5, 7\}$ and $\{3, 9, 15, 21\}$ are reduced sets of residues modulo 8.

We denote the group of units in $\mathbf{Z}/m\mathbf{Z}$ by

$$(\mathbf{Z}/m\mathbf{Z})^{\times}.$$

If $R = \{r_1, \ldots, r_{\varphi(m)}\}$ is a reduced set of residues modulo m, then

$$(\mathbf{Z}/m\mathbf{Z})^{\times} = \{r + m\mathbf{Z} : r \in R\}$$

and

$$\left|(\mathbf{Z}/m\mathbf{Z})^{\times}\right| = \varphi(m).$$

For example,

$$(\mathbf{Z}/6\mathbf{Z})^{\times} = \{1 + 6\mathbf{Z}, 5 + 6\mathbf{Z}\}$$

and

$$(\mathbf{Z}/7\mathbf{Z})^{\times} = \{1 + 7\mathbf{Z}, 2 + 7\mathbf{Z}, 3 + 7\mathbf{Z}, 4 + 7\mathbf{Z}, 5 + 7\mathbf{Z}, 6 + 7\mathbf{Z}\}.$$

If $a + m\mathbf{Z}$ is a unit in $\mathbf{Z}/m\mathbf{Z}$, then $(a, m) = 1$ and we can apply the Euclidean algorithm to compute $(a + m\mathbf{Z})^{-1}$. If we can find integers x and y such that

$$ax + my = 1,$$

then

$$(a + m\mathbf{Z})(x + m\mathbf{Z}) = 1 + m\mathbf{Z},$$

and $x + m\mathbf{Z} = (a + m\mathbf{Z})^{-1}$.

For example, to find the inverse of $13 + 17\mathbf{Z}$, we use the Euclidean algorithm to obtain

$$\begin{aligned} 17 &= 13 \cdot 1 + 4, \\ 13 &= 4 \cdot 3 + 1, \\ 4 &= 1 \cdot 4. \end{aligned}$$

This gives

$$1 = 13 - 4 \cdot 3 = 13 - (17 - 13 \cdot 1)3 = 13 \cdot 4 - 17 \cdot 3,$$

and so

$$13 \cdot 4 \equiv 1 \pmod{17}.$$

Therefore,

$$(13 + 17\mathbf{Z})^{-1} = 4 + 17\mathbf{Z}.$$

2.3 The Euler Phi Function

An *arithmetic function* is a function defined on the positive integers. The Euler phi function $\varphi(m)$ is the arithmetic function that counts the number of integers in the set $0, 1, 2, \ldots, m-1$ that are relatively prime to m. We have

$$\begin{array}{lcllcl} \varphi(1) & = & 1, & \varphi(6) & = & 2, \\ \varphi(2) & = & 2, & \varphi(7) & = & 6, \\ \varphi(3) & = & 3, & \varphi(8) & = & 4, \\ \varphi(4) & = & 2, & \varphi(9) & = & 6, \\ \varphi(5) & = & 4, & \varphi(10) & = & 4. \end{array}$$

If p is a prime number, then $(a, p) = 1$ for $a = 1, \ldots, p-1$, and $\varphi(p) = p-1$. If p^r is a prime power and $0 \leq a \leq p^r - 1$, then $(a, p^r) > 1$ if and only if a is a multiple of p. The integral multiples of p in the interval $[0, p^r - 1]$ are the p^{r-1} numbers $0, p, 2p, 3p, \ldots, (p^{r-1} - 1)p$, and so

$$\varphi(p^r) = p^r - p^{r-1} = p^r \left(1 - \frac{1}{p}\right).$$

In this section we shall obtain some important properties of the Euler phi function.

Theorem 2.6 *Let m and n be relatively prime positive integers. For every integer c there exist unique integers a and b such that*

$$0 \leq a \leq n-1,$$

$$0 \leq b \leq m-1,$$

and

$$c \equiv ma + nb \pmod{mn}. \tag{2.4}$$

Moreover, $(c, mn) = 1$ if and only if $(a, n) = (b, m) = 1$ in the representation (2.4).

Proof. If a_1, a_2, b_1, b_2 are integers such that

$$ma_1 + nb_1 \equiv ma_2 + nb_2 \pmod{mn},$$

then

$$ma_1 \equiv ma_1 + nb_1 \equiv ma_2 + nb_2 \equiv ma_2 \pmod{n}.$$

Since $(m, n) = 1$, it follows that

$$a_1 \equiv a_2 \pmod{n},$$

and so $a_1 = a_2$. Similarly, $b_1 = b_2$. It follows that the mn integers $ma + nb$ are pairwise incongruent modulo mn. Since there are exactly mn distinct congruence classes modulo mn, the congruence (2.4) has a unique solution for every integer c.

Let $c \equiv ma + nb \pmod{mn}$. Since $(m, n) = 1$, we have

$$(c, m) = (ma + nb, m) = (nb, m) = (b, m)$$

and

$$(c, n) = (ma + nb, n) = (ma, n) = (a, n).$$

It follows that $(c, mn) = 1$ if and only if $(c, m) = (c, n) = 1$ if and only if $(b, m) = (a, n) = 1$. This completes the proof. □

For example, we can represent the congruence classes modulo 6 as linear combinations of 2 and 3 as follows:

$$\begin{aligned}
0 &\equiv 0 \cdot 2 + 0 \cdot 3 \pmod 6, \\
1 &\equiv 2 \cdot 2 + 1 \cdot 3 \pmod 6, \\
2 &\equiv 1 \cdot 2 + 0 \cdot 3 \pmod 6, \\
3 &\equiv 0 \cdot 2 + 1 \cdot 3 \pmod 6, \\
4 &\equiv 2 \cdot 2 + 0 \cdot 3 \pmod 6, \\
5 &\equiv 1 \cdot 2 + 1 \cdot 3 \pmod 6.
\end{aligned}$$

A *multiplicative* function is an arithmetic function $f(m)$ such that $f(mn) = f(m)f(n)$ for all pairs of relatively prime positive integers m and n. If $f(m)$ is multiplicative, then it is easy to prove by induction on k that if $m_1, \ldots, m_k$ are pairwise relatively prime positive integers, then $f(m_1 \cdots m_k) = f(m_1) \cdots f(m_k)$.

Theorem 2.7 *The Euler phi function is multiplicative. Moreover,*

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right).$$

Proof. Let $(m, n) = 1$. There are $\varphi(mn)$ congruence classes in the ring $\mathbf{Z}/mn\mathbf{Z}$ that are relatively prime to mn. By Theorem 2.6, every congruence class modulo mn can be written uniquely in the form $ma + nb + mn\mathbf{Z}$, where a and b are integers such that $0 \leq a \leq n-1$ and $0 \leq b \leq m-1$. Moreover, the congruence class $ma + nb + mn\mathbf{Z}$ is prime to mn if and only if $(b, m) = (a, n) = 1$. Since there are $\varphi(n)$ integers $a \in [0, n-1]$ that are relatively prime to n, and $\varphi(m)$ integers $b \in [0, m-1]$ relatively prime to m, it follows that $\varphi(mn) = \varphi(m)\varphi(n)$, and so the Euler phi function is multiplicative. If $m_1, \ldots, m_k$ are pairwise relatively prime positive integers, then $\varphi(m_1 \cdots m_k) = \varphi(m_1) \cdots \varphi(m_k)$. In particular, if $m = p_1^{r_1} \cdots p_k^{r_k}$ is the standard factorization of m, where $p_1, \ldots, p_k$ are distinct primes and $r_1, \ldots, r_k$ are positive integers, then

$$\varphi(m) = \prod_{i=1}^{k} \varphi\left(p_i^{r_i}\right) = \prod_{i=1}^{k} p_i^{r_i}\left(1 - \frac{1}{p_i}\right) = m \prod_{p|m}\left(1 - \frac{1}{p}\right).$$

This completes the proof. □

For example, $7875 = 3^2 5^3 7$ and

$$\varphi(7875) = \varphi(3^2)\varphi(5^3)\varphi(7) = (9-3)(125-25)(7-1) = 3600.$$

Theorem 2.8 *For every positive integer m,*

$$\sum_{d|m} \varphi(d) = m.$$

Proof. We first consider the case where $m = p^t$ is a power of a prime p. The divisors of p^t are $1, p, p^2, \ldots, p^t$, and

$$\sum_{d|p^t} \varphi(d) = \sum_{r=0}^{t} \varphi(p^r) = 1 + \sum_{r=1}^{t} \left(p^r - p^{r-1}\right) = p^t.$$

Next we consider the general case where m has the standard factorization

$$m = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k},$$

where $p_1, \ldots, p_k$ are distinct prime numbers and $t_1, \ldots, t_k$ are positive integers. Every divisor d of m is of the form

$$d = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k},$$

where $0 \leq r_i \leq t_i$ for $i = 1, \ldots, k$. By Theorem 2.7, $\varphi(d)$ is multiplicative, and so

$$\varphi(d) = \varphi(p_1^{r_1})\varphi(p_2^{r_2}) \cdots \varphi(p_k^{r_k}).$$

Therefore,

$$\begin{aligned}
\sum_{d|m} \varphi(d) &= \sum_{r_1=0}^{t_1} \cdots \sum_{r_k=0}^{t_k} \varphi\left(p_1^{r_1} \cdots p_k^{r_k}\right) \\
&= \sum_{r_1=0}^{t_1} \cdots \sum_{r_k=0}^{t_k} \varphi(p_1^{r_1}) \varphi(p_2^{r_2}) \cdots \varphi(p_k^{r_k}) \\
&= \prod_{i=1}^{k} \sum_{r_i=0}^{t_i} \varphi\left(p_i^{r_i}\right) \\
&= \prod_{i=1}^{k} p_i^{t_i} \\
&= m.
\end{aligned}$$

This completes the proof. □

For example,

$$\begin{aligned}\sum_{d|12}\varphi(d) &= \varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(6)+\varphi(12)\\ &= 1+1+2+2+2+4\\ &= 12\end{aligned}$$

and

$$\begin{aligned}\sum_{d|45}\varphi(d) &= \varphi(1)+\varphi(3)+\varphi(5)+\varphi(9)+\varphi(15)+\varphi(45)\\ &= 1+2+4+6+8+24\\ &= 45.\end{aligned}$$

2.4 Chinese Remainder Theorem

Theorem 2.9 *Let m and n be positive integers. For any integers a and b there exists an integer x such that*

$$x \equiv a \pmod{m} \tag{2.5}$$

and

$$x \equiv b \pmod{n} \tag{2.6}$$

if and only if

$$a \equiv b \pmod{(m,n)}.$$

If x is a solution of congruences (2.5) and (2.6), then the integer y is also a solution if and only if

$$x \equiv y \pmod{[m,n]}.$$

Proof. If x is a solution of congruence (2.5), then $x = a + mu$ for some integer u. If x is also a solution of congruence (2.6), then

$$x = a + mu \equiv b \pmod{n},$$

that is,

$$a + mu = b + nv$$

for some integer v. It follows that

$$a - b = nv - mu \equiv 0 \pmod{(m, n)}.$$

Conversely, if $a - b \equiv 0 \pmod{(m, n)}$, then by Theorem 1.15 there exist integers u and v such that

$$a - b = nv - mu.$$

Then

$$x = a + mu = b + nv$$

is a solution of the two congruences.

An integer y is another solution of the congruences if and only if

$$y \equiv a \equiv x \pmod{m}$$

and

$$y \equiv b \equiv x \pmod{n},$$

that is, if and only if $x-y$ is a common multiple of m and n, or, equivalently, $x - y$ is divisible by the least common multiple $[m, n]$. This completes the proof. $\square$

For example, the system of congruences

$$\begin{aligned} x &\equiv 5 \pmod{21}, \\ x &\equiv 19 \pmod{56}, \end{aligned}$$

has a solution, since

$$(56, 21) = 7$$

and

$$19 \equiv 5 \pmod{7}.$$

The integer x is a solution if there exists an integer u such that

$$x = 5 + 21u \equiv 19 \pmod{56},$$

that is,

$$21u \equiv 14 \pmod{56},$$

$$3u \equiv 2 \pmod{8},$$

or

$$u \equiv 6 \pmod{8}.$$

Then

$$x = 5 + 21u = 5 + 21(6 + 8v) = 131 + 168v$$

is a solution of the system of congruences for any integer v, and so the set of all solutions is the congruence class $131 + 168\mathbf{Z}$.

Theorem 2.10 (Chinese remainder theorem) *Let $k \geq 2$. If $a_1, \ldots, a_k$ are integers and $m_1, \ldots, m_k$ are pairwise relatively prime positive integers, then there exists an integer x such that*

$$x \equiv a_i \pmod{m_i} \quad \text{for all } i = 1, \ldots, k.$$

If x is any solution of this set of congruences, then the integer y is also a solution if and only if

$$x \equiv y \pmod{m_1 \cdots m_k}.$$

Proof. We prove the theorem by induction on k. If $k = 2$, then $[m_1, m_2] = m_1 m_2$, and this is a special case of Theorem 2.9.

Let $k \geq 3$, and assume that the statement is true for $k-1$ congruences. Then there exists an integer z such that $z \equiv a_i \pmod{m_i}$ for $i = 1, \ldots, k-1$. Since $m_1, \ldots, m_k$ are pairwise relatively prime integers, we have

$$(m_1 \cdots m_{k-1}, m_k) = 1,$$

and so, by the case $k = 2$, there exists an integer x such that

$$\begin{aligned} x &\equiv z \pmod{m_1 \cdots m_{k-1}}, \\ x &\equiv a_k \pmod{m_k}. \end{aligned}$$

Then

$$x \equiv z \equiv a_i \pmod{m_i}$$

for $i = 1, \ldots, k-1$.

If y is another solution of the system of k congruences, then $x - y$ is divisible by m_i for all $i = 1, \ldots, k$. Since $m_1, \ldots, m_k$ are pairwise relatively prime, it follows that $x - y$ is divisible by $m_1 \cdots m_k$. This completes the proof. □

For example, the system of congruences

$$\begin{aligned} x &\equiv 2 \pmod 3, \\ x &\equiv 3 \pmod 5, \\ x &\equiv 5 \pmod 7, \\ x &\equiv 7 \pmod{11} \end{aligned}$$

has a solution, since the moduli are pairwise relatively prime. The solution to the first two congruences is the congruence class

$$x \equiv 8 \pmod{15}.$$

The solution to the first three congruences is the congruence class

$$x \equiv 68 \pmod{105}.$$

The solution to the four congruences is the congruence class

$$x \equiv 1118 \pmod{1155}.$$

There is an important application of the Chinese remainder theorem to the problem of solving diophantine equations of the form

$$f(x_1, \ldots, x_k) \equiv 0 \pmod{m},$$

where $f(x_1, \ldots, x_k)$ is a polynomial with integer coefficients in one or several variables. This equation is *solvable modulo* m if there exist integers $a_1, \ldots, a_k$ such that

$$f(a_1, \ldots, a_k) \equiv 0 \pmod{m}.$$

The Chinese remainder theorem allows us to reduce the question of the solvability of this congruence modulo m to the special case of prime power moduli p^r. For simplicity, we consider polynomials in only one variable.

Theorem 2.11 *Let*

$$m = p_1^{r_1} \cdots p_k^{r_k}$$

be the standard factorization of the positive integer m. Let $f(x)$ be a polynomial with integral coefficients. The congruence

$$f(x) \equiv 0 \pmod{m}$$

is solvable if and only if the congruences

$$f(x) \equiv 0 \pmod{p_i^{r_i}}$$

are solvable for all $i = 1, \ldots, k$.

Proof. If $f(x) \equiv 0 \pmod{m}$ has a solution in integers, then there exists an integer a such that m divides $f(a)$. Since $p_i^{r_i}$ divides m, it follows that $p_i^{r_i}$ divides $f(a)$, and so the congruences $f(x) \equiv 0 \pmod{p_i^{r_i}}$ are solvable for $i = 1, \ldots, k$.

Conversely, suppose that the congruences $f(x) \equiv 0 \pmod{p_i^{r_i}}$ are solvable for $i = 1, \ldots, k$. Then for each i there exists an integer a_i such that

$$f(a_i) \equiv 0 \pmod{p_i^{r_i}}.$$

Since the prime powers $p_1^{r_1}, \ldots, p_k^{r_k}$ are pairwise relatively prime, the Chinese remainder theorem tells us that there exists an integer a such that

$$a \equiv a_i \pmod{p_i^{r_i}}$$

for all i. Then

$$f(a) \equiv f(a_i) \equiv 0 \pmod{p_i^{r_i}}$$

for all i. Since $f(a)$ is divisible by each of the prime powers $p_i^{r_i}$, it is also divisible by their product m, and so $f(a) \equiv 0 \pmod{m}$. This completes the proof. $\square$

For example, consider the congruence

$$f(x) = x^2 - 34 \equiv 0 \pmod{495}.$$

Since $495 = 3^2 \cdot 5 \cdot 11$, it suffices to solve the congruences

$$f(x) = x^2 - 34 \equiv x^2 + 2 \equiv 0 \pmod{9},$$

$$f(x) = x^2 - 34 \equiv x^2 + 1 \equiv 0 \pmod{5},$$

and

$$f(x) = x^2 - 34 \equiv x^2 - 1 \equiv 0 \pmod{11}.$$

These congruences have solutions

$$f(5) \equiv 0 \pmod{9},$$

$$f(2) \equiv 0 \pmod{5},$$

and

$$f(1) \equiv 0 \pmod{11}.$$

By the Chinese remainder theorem, there exists an integer a such that

$$\begin{aligned} a &\equiv 5 \pmod 9, \\ a &\equiv 2 \pmod 5, \\ a &\equiv 1 \pmod{11}. \end{aligned}$$

Solving these congruences, we obtain

$$a \equiv 122 \pmod{495}.$$

We can check that

$$f(122) = 122^2 - 34 = 14,850 = 30 \cdot 495,$$

and so

$$f(122) \equiv 0 \pmod{495}.$$

2.5 Euler's Theorem and Fermat's Theorem

Theorem 2.12 (Euler) *Let m be a positive integer, and let a be an integer relatively prime to m. Then*

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

Proof. Let $\{r_1, \ldots, r_{\varphi(m)}\}$ be a reduced set of residues modulo m. Since $(a, m) = 1$, we have $(ar_i, m) = 1$ for $i = 1, \ldots, \varphi(m)$. Consequently, for every $i \in \{1, \ldots, \varphi(m)\}$ there exists $\sigma(i) \in \{1, \ldots, \varphi(m)\}$ such that

$$ar_i \equiv r_{\sigma(i)} \pmod{m}.$$

Moreover, $ar_i \equiv ar_j \pmod{m}$ if and only if $i = j$, and so σ is a permutation of the set $\{1, \ldots, \varphi(m)\}$ and $\{ar_1, \ldots, ar_{\varphi(m)}\}$ is also a reduced set of residues modulo m. It follows that

$$\begin{aligned} a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} &\equiv (ar_1)(ar_2)\cdots(ar_{\varphi(m)}) \pmod{m} \\ &\equiv r_{\sigma(1)} r_{\sigma(2)} \cdots r_{\sigma(\varphi(m))} \pmod{m} \\ &\equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m}. \end{aligned}$$

Dividing by $r_1 r_2 \cdots r_{\varphi(m)}$, we obtain

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

This completes the proof. □

Theorem 2.13 (Fermat) *Let p be a prime number. If the integer a is not divisible by p, then*

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

Moreover,

$$a^p \equiv a \pmod{p}$$

for every integer a.

Proof. If p is prime and does not divide a, then $(a, p) = 1$, $\varphi(p) = p - 1$, and

$$a^{p-1} = a^{\varphi(p)} \equiv 1 \pmod{p}$$

by Euler's theorem. Multiplying this congruence by a, we obtain

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

If p divides a, then this congruence also holds for a. □

Let m be a positive integer and let a be an integer that is relatively prime to m. By Euler's theorem, $a^{\varphi(m)} \equiv 1 \pmod{m}$. The *order* of a with respect to the modulus m is the smallest positive integer d such that $a^d \equiv 1 \pmod{m}$. Then $1 \leq d \leq \varphi(m)$. We denote the order of a modulo m by $\mathrm{ord}_m(a)$. We shall prove that $\mathrm{ord}_m(a)$ divides $\varphi(m)$ for every integer a relatively prime to p.

Theorem 2.14 *Let m be a positive integer and a an integer relatively prime to m. If d is the order of a modulo m, then $a^k \equiv a^\ell \pmod{m}$ if and only if $k \equiv \ell \pmod{d}$. In particular, $a^n \equiv 1 \pmod{m}$ if and only if d divides n, and so d divides $\varphi(m)$.*

Proof. Since a has order d modulo m, we have $a^d \equiv 1 \pmod{m}$. If $k \equiv \ell \pmod{d}$, then $k = \ell + dq$, and so

$$a^k = a^{\ell+dq} = a^\ell \left(a^d\right)^q \equiv a^\ell \pmod{m}.$$

Conversely, suppose that $a^k \equiv a^\ell \pmod{m}$. By the division algorithm, there exist integers q and r such that

$$k - \ell = dq + r \qquad \text{and} \qquad 0 \leq r \leq d - 1.$$

Then

$$a^k = a^{\ell+dq+r} = a^\ell \left(a^d\right)^q a^r \equiv a^k a^r \pmod{m}.$$

Since $(a^k, m) = 1$, we can divide this congruence by a^k and obtain

$$a^r \equiv 1 \pmod{m}.$$

Since $0 \leq r \leq d-1$, and d is the order of a modulo m, it follows that $r = 0$, and so $k \equiv \ell \pmod{d}$.

If $a^n \equiv 1 \equiv a^0 \pmod{m}$, then d divides n. In particular, d divides $\varphi(m)$, since $a^{\varphi(m)} \equiv 1 \pmod{m}$ by Euler's theorem. $\square$

thank you

Introduction to number theory

Lecturers (30 hours): Maciej Zakarczemny

Exercises (problem sessions 15 hours): Maciej Zakarczemny

Assessment method: two tests during the semester, final exam

The first exam is scheduled for Monday, 26 June 2017, 14.00 – 15:00.

Lectures and a lists of exercises (exercises sheets) will be available online.

My website: maciej.zakarczemny.pl

tab: Introduction to number theory

Topics covered:

Notation and Conventions

Divisibility, GCD, factorization

Fundamental Theorem of Arithmetic

Congruences

Fermat's Little Theorem

Euler's Phi function.

Prime numbers; counting primes, Mersenne and other types of primes

Carmichael numbers

Modular arithmetic and algebra, Chinese Remainder Theorem.

Diophantine equations.

Pythagorean Triples and the Fermat's Last Theorem

"Unbreakable" codes and other applications.

Books:

J. Silverman, A friendly introduction to Number Theory, Prentice Hall, 1997.

Shoup, V. A Computational Introduction to Number Theory and Algebra.

Available at: http://shoup.net/ntb/ntb-v2.pdf

K. Ireland, M. Rosen, A classical introduction in modern number theory, Springer 1990.

W.Narkiewicz, Number Theory, World Scientific, Singapore, 1983.

W.Sierpiński. Elementary theory of numbers, Warszawa-Amsterdam-New York-Oxford 1987.

Z.I. Borevich. I.R.Shafarevich, Number Theory, Academic Press 1966

H. Davenport, The Higher Arithmetic, Cambridge University Press.

G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers,
Oxford University Press, 1979.

Requirements to pass the lectures and exercises.

General notes regarding the course:

To pass the course, you need to pass the final exam in the end,

and you need to pass the exercises.

Students must score at least 60 percent on the exam to pass.

Requirements to pass the lectures and exercises.

General notes regarding the course:

To pass the exercises you need to pass:

homework exercises (which will be put on the webpage in due course)

and two tests.

Minimum passing is 60 percent.

The maximum number of lessons that a student may

be absent without acceptable documentation justifying the absence is 2.

Class attendance is required of all undergraduates unless the student has

an official excused absence.

Excused absences are granted for one general reason:

Student has a documented personal reason (illness, injury, health condition etc.).

Consultation hours: Monday 13.30 - 14.30

Room 304/14, located on the third floor, building WIEiK

e-mail: mzakarczemny@pk.edu.pl