First Arts Modular Degree

Lecture Notes 2004–2005

Chapter 3: Congruences and Congruence Classes

(3.1) Definition Let n be a non-zero integer. If a and b are integers, we say that a and b are *congruent* modulo n if n exactly divides $b - a$. We write

$$a \equiv b \bmod n$$

to signify that a and b are congruent modulo n.

Thus $a \equiv b \bmod n$ means that $b - a$ must be a multiple of n (as n is an exact divisor of $b - a$) and so $b = a + cn$ for some integer c. Notice that if $a \equiv b \bmod n$, then it is also true that $b \equiv a \bmod n$. Thus, we can interchange order in congruences.

Examples

(a) Taking n equal to 2, integers a and b are congruent modulo 2 precisely when a and b are both even or both odd (an integer is even if it is divisible by 2, odd if it is not divisible by 2).
(b) Observe the simple congruences $13 \equiv 5 \bmod 8$, and $2 \equiv -1 \bmod 3$.

The property of congruence of integers has many similarities with the property of equality of integers, as we intend to prove now.

(3.2) Theorem Let n be a non-zero integer and let a and b be integers. Then we have the following.

(i) If $a \equiv b \bmod n$, then $ka \equiv kb \bmod n$ for all integers k.
(ii) If $a \equiv b \bmod n$ and $b \equiv c \bmod n$, then $a \equiv c \bmod n$.
(iii) If $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$, then $a + b \equiv a' + b' \bmod n$ and $ab \equiv a'b' \bmod n$.
(iv) If $a \equiv b \bmod n$ and t is a positive integer $a^t \equiv b^t \bmod n$.

Proof (i) Suppose that $a \equiv b \bmod n$. Then we have

$$b - a = sn$$

for some integer s. If k is any integer, we obtain

$$kb - ka = ksn$$

on multiplying the equation above by k. But this equation says that n divides the difference $kb - ka$ and so $ka \equiv kb \bmod n$.

(ii) Suppose next that If $a \equiv b \bmod n$ and $b \equiv c \bmod n$. Then it follows that

$$b - a = un, \quad c - b = sn$$

for suitable integers u and s. Adding the two equations we get

$$c - b + b - a = c - a = un + sn = (u + s)n,$$

so that n divides $c - b$. Hence $a \equiv c \bmod n$.

(iii) Suppose that If $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$. By definition,

$$a' - a = rn, \quad b' - b = qn$$

for suitable integers r and q. Adding these equations, we get

$$a' - a + b' - b = (a' + b') - (a + b) = (r + q)n$$

and this implies that

$$a + b \equiv a' + b' \bmod n.$$

We can also write

$$a' = a + rn, \quad b' = b + qn$$

and by multiplication we get

$$\begin{aligned} a'b' = (a + rn)(b + qn) &= ab + rbn + aqn + rqn^2 \\ &= ab + (rb + aq + rqn)n. \end{aligned}$$

This shows that n divides $a'b' - ab$, so that $a'b' \equiv ab \bmod n$.

(iv) We proceed by induction on t. The result is obvious if $t = 1$. Suppose then that $a^r \equiv b^r \bmod n$. We need to prove that $a^{r+1} \equiv b^{r+1} \bmod n$. But if in part (iii) we replace a by a^r, b by b^r, a' by a and b' by b, we get $a^r a \equiv b^r b \bmod n$ and this proves what we want. ■

Sometimes the study of integers leads us to seek solutions of congruences of the form

$$bx \equiv c \bmod n,$$

where b, c and n are given integers, and we are looking for an integer x that solves the problem.

<u>(3.3) Lemma</u> Let b, c and n be integers, with n non-zero. Then there exists an integer solution x to the congruence $bx \equiv c \bmod n$ if and only if the gcd of b and n divides c.

<u>Proof</u> Let $d = \gcd(b, n)$. Suppose that there exists an integer x that satisfies the congruence. Then there exists an integer e with

$$bx - c = en.$$

Now d divides b, and hence bx, and also divides en. Thus d divides $bx - en = c$, as required.

Conversely, suppose that d divides c, and put $c = fd$ for some integer f. By Euclid's algorithm, we can find integers s and t so that

$$sb + tn = d.$$

Multiplying by f, we get $fsb + ftn = fd = c$. Thus n divides $fsb - c$ and hence

$$fsb \equiv c \bmod n.$$

If we take $x = fs$, we get an integer solution to the congruence. ■

Note that having found the solution x as above, any integer x' with $x' \equiv x \bmod n$ will also solve the congruence. Then, if we want the *smallest positive* solution, we find the unique positive integer r lying between 0 and $n-1$ that satisfies $x \equiv r \bmod n$, and then this r will give the smallest positive solution. (In other words, r is the remainder on dividing x by n.)

<u>Examples</u>

(a) There is no integer solution x to the congruence $12x \equiv 7 \bmod 21$, since the gcd of 12 and 21 is 3 and 3 does not divide 7.

(b) There is an integer solution to $12x \equiv 17 \bmod 35$, since 12 and 35 are relatively prime. Performing the Euclidean algorithm, we get

$$35 = 2 \times 12 + 11, \quad 12 = 11 + 1.$$

So, $1 = 12 - 11 = 12 - (35 - 2 \times 12) = (3 \times 12) - 35$. Multiplying by 17, we get $17 = (51 \times 12) - (17 \times 35)$ and thus we may take $x = 51$. By the remark above, x' with $x' \equiv 51 \bmod 35$ will also give a solution and so we may take $x' = 16$ as a smaller solution.

(c) $99x \equiv 5 \bmod 221$. Clearly, 99 and 221 are relatively prime, and thus we may solve the congruence. We have

$$1 = 7 - 2 \times 3$$

$$2 = 23 - 7 \times 3$$

$$7 = 99 - 4 \times 23$$

$$23 = 221 - 2 \times 99$$

This leads to

$$1 = 10 \times 7 - 3 \times 23$$

$$1 = 10 \times 99 - 43 \times 23$$

$$1 = 96 \times 99 - 43 \times 221$$

Hence

$$5 = 5 \times 96 \times 99 - 43 \times 221 \times 5$$

which gives $99(5 \times 96) \equiv 5 \bmod 221$. We may thus take $x = 5 \times 96 = 480$ as a solution. As $480 = 2 \times 221 + 38$, we get $x = 38$ as the smallest positive solution.

Example Find the smallest positive integer x that satisfies $169x \equiv 5 \bmod 408$.

We have

$$1 = 5 - 2 \times 2$$

$$2 = 12 - 2 \times 5$$

$$5 = 29 - 2 \times 12$$

$$12 = 70 - 2 \times 29$$

$$29 = 169 - 2 \times 70$$

$$70 = 408 - 2 \times 169$$

This leads to

$$1 = 5 \times 5 - 2 \times 12$$

$$1 = 5 \times 29 - 12 \times 12$$

$$1 = 29 \times 169 - 70 \times 70$$

$$1 = 169 \times 169 - 70 \times 408.$$

This gives

$$169 \times 169 \equiv 1 \bmod 408.$$

Multiplying by 5 we get

$$169 \times (169 \times 5) \equiv 5 \bmod 408.$$

This shows that $x = 169 \times 5 = 845$ will solve the congruence. As 845 is larger than 408, we remove multiples of 408 to make the answer smaller. Now

$$x \equiv 29 \bmod 408$$

and so $x = 29$ is the smallest positive solution.

In the theory of congruence, the modulus most frequently used is a prime integer, and it is congruences modulo a prime that we will discuss now. Recall that the binomial coefficient $\binom{n}{m}$ is defined by

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}.$$

While it is not obvious from this definition, the binomial coefficients are integers. This follows, for example, from the fact that $\binom{n}{m}$ counts the number of subsets of size m in a set of size n.

<u>(3.4) Lemma</u> Let p be a prime. Then p divides $\binom{p}{m}$ for $1 \leq m \leq p-1$.

<u>Proof</u> We show that

$$m\binom{p}{m} = p\binom{p-1}{m-1}.$$

Now

$$m\binom{p}{m} = m\frac{p!}{m!(p-m)!} = \frac{p!}{(m-1)!(p-m)!}$$

and

$$p\binom{p-1}{m-1} = \frac{p(p-1)!}{(m-1)!(p-1-(m-1))!} = \frac{p!}{(m-1)!(p-m)!}$$

This proves what we want. Thus p divides $m\binom{p}{m}$. By Theorem 2.14, p divides m or p divides $\binom{p}{m}$. But if $1 \leq m \leq p-1$, p cannot divide m, as it is too large. Thus p divides $\binom{p}{m}$, as required. ■

Now we can move to the proof of an important result in the theory of congruence modulo a prime.

<u>(3.5) Theorem</u> Let p be a prime and let n be a positive integer. Then $n^p \equiv n \bmod p$.

<u>Proof</u> We prove this result by induction on n. The theorem is clear if $n = 1$. Suppose then that $r^p \equiv r \bmod p$. We wish then to prove that $(r+1)^p \equiv r+1 \bmod p$. By the binomial theorem,

$$(r+1)^p = 1^p + \binom{p}{1}r + \cdots + \binom{p}{i}r^i + \cdots + \binom{p}{p-1}r^{p-1} + r^p.$$

By Lemma 3.4, p divides each binomial coefficient $\binom{p}{i}$ for $1 \leq i \leq p-1$ and thus

$$(r+1)^p \equiv r^p + 1 \bmod p,$$

by properties of congruences. But $r^p \equiv r \bmod p$, by induction and thus $(r+1)^p \equiv r+1 \bmod p$. ■

(3.6) Corollary (Fermat's Little Theorem) Let p be a prime and let n be a positive integer. Suppose that p does not divide n. Then $n^{p-1} \equiv 1 \bmod p$.

Proof We have seen that

$$n^p \equiv n \bmod p$$

and thus p divides $n^p - n = n(n^{p-1} - 1)$. By Theorem 2.14, p divides one of n and $n^{p-1} - 1$. The first case is ruled out and thus p divides $n^{p-1} - 1$. This of course implies the desired result. ■

The main force of Fermat's Little Theorem is that it enables us to investigate congruences without the need to perform complicated multiplication processes.

Examples

(a) Show that $9^5 - 4^5$ is divisible by 11. Now $9 = 3^2$ and so $9^5 = 3^{10} \equiv 1 \bmod 11$. Similarly, $4 = 2^2$ and so $4^5 = 2^{10} \equiv 1 \bmod 11$. Therefore,

$$9^5 - 4^5 \equiv 1 - 1 \equiv 0 \bmod 11,$$

giving what we want.

(b) Find the smallest positive integer x so that $2^{58} \equiv x \bmod 53$. Now as 53 is a prime, we have

$$2^{52} \equiv 1 \bmod 53,$$

by Fermat's Little Theorem. Thus,

$$2^{58} \equiv 2^6 \equiv 64 \bmod 53.$$

But $64 \equiv 11 \bmod 53$ and we therefore take $x = 11$ as the solution to the congruence.

(c) Find the smallest positive integer a satisfying $3^{44} \equiv a \bmod 47$.

By FLT, we have $3^{46} \equiv 1 \bmod 47$, since 47 is a prime. Thus if $3^{44} \equiv a \bmod 47$, it follows that $3^{46} \equiv 9a \equiv 1 \bmod 47$. Thus a is a solution of $9a \equiv 1 \bmod 47$. By calculation,

$$1 = 9 - 4 \times 2, \quad 2 = 47 - 5 \times 9$$

which shows that $1 = 21 \times 9 - 4 \times 47$. Hence $9 \times 21 \equiv 1 \bmod 47$ and since $0 < 21 < 47$, 21 is the required solution.

<u>(3.7) Definition</u> Let p be a prime and let n be a positive integer not divisible by p. The *smallest* positive integer m with $n^m \equiv 1 \bmod p$ is called the *order* of n modulo p.

Note that Fermat's Little Theorem shows that the order of n modulo p is at most $p-1$. However, we can improve this observation, as we now show.

<u>(3.8) Theorem</u> Let p be a prime and let n be a positive integer not divisible by p. Suppose that for some positive integer k, we have $n^k \equiv 1 \bmod p$. Then the order of n modulo p is a divisor of k. Thus, in particular, the order of n modulo p is a divisor of $p-1$.

<u>Proof</u> Let m be the order of n modulo p. By the division algorithm, we may write

$$k = mq + r,$$

where $0 \leq r < m$. We want to show that $r = 0$, which implies that m is an exact divisor of k. Now we have

$$n^k = n^{mq} n^r$$

and as m is the order of n modulo p,

$$n^m \equiv 1 \bmod p$$

Raising each side to the power q, we obtain

$$(n^m)^q \equiv 1^q \equiv 1 \bmod p$$

and thus

$$n^{mq} \equiv 1 \bmod p$$

Then by Theorem 3.2 (i), we may multiply each side of this congruence by n^r to obtain

$$n^{mq} n^r \equiv 1 \cdot n^r \bmod p \text{ and hence } n^k \equiv n^r \bmod p.$$

Since $n^k \equiv 1 \bmod p$ by assumption, we obtain $n^r \equiv 1 \bmod p$. As r is non-negative and less than m, the minimality of m forces the conclusion that $r = 0$. This means that m divides k, as required. Finally, since $n^{p-1} \equiv 1 \bmod p$, by Fermat's Little Theorem, we obtain that m divides $p-1$ by taking $k = p-1$. ∎

Examples

(a) Find the order of 2 modulo 23. Now 23 is a prime and it follows that the order is a divisor of 23-1=22. There is no better way to find the order than to check the divisors of 22 in turn. Now the order is clearly not 1 or 2, so it can only be 11 or 22. We have

$$2^5 = 32 \equiv 9 \bmod 23, \quad 2^{10} \equiv 9^2 \equiv 81 \equiv 12 \bmod 23.$$

Therefore, $2^{11} \equiv 24 \equiv 1 \bmod 23$ and we see that the order is 11.

(b) Find the order of 3 modulo 41. Here again, 41 is a prime and so the order is a divisor of 40, hence one of 2, 4, 8, 5, 10, 20 and 40.

$$3^2 \equiv 9 \bmod 41, \quad 3^4 \equiv 81 \equiv -1 \bmod 41.$$

Now it is easier to work with the negative integer -1 rather than 40, since $-1 \equiv 40 \bmod 41$. Thus $3^8 \equiv (-1)^2 = 1 \bmod 41$ and we see that 3 has order 8 modulo 41. The order can't be 5, as five is not a divisor of 8.

For our next topic, we will consider a generalization of Fermat's Little Theorem.

(3.9) Definition Let n be an integer greater than 1. Then we define $\varphi(n)$ to be the number of integers b that satisfy

$$1 \leq b < n \text{ and } \gcd(b, n) = 1.$$

We call φ the *Euler function* and we will work out a way later to calculate $\varphi(n)$ from a knowledge of the prime factorization of n.

Example Take $n = 12$. The prime divisors of 12 are 2 and 3, so an integer is relatively prime to 12 if it is not divisible by either 2 or 3. The only integers lying between 1 and 12 that are not divisible by 2 or 3 are 1, 5, 7, 11 and it follows that $\varphi(12) = 4$.

(3.10) Lemma Let c_1, c_2, $\ldots$, $c_{\varphi(n)}$ denote the $\varphi(n)$ different integers lying between 1 and n that are relatively prime to n and let b be any integer relatively prime to n. Form the $\varphi(n)$ products

$$bc_1, bc_2, \ldots, bc_{\varphi(n)}$$

and for each i, let r_i be the remainder when bc_i is divided by n. Then r_1, r_2, $\ldots$, $r_{\varphi(n)}$ are just c_1, c_2, $\ldots$, $c_{\varphi(n)}$ in some rearranged order.

Proof For simplicity, write $\varphi(n) = m$. We have now

$$\begin{aligned} bc_1 &= q_1 n + r_1 \\ bc_2 &= q_2 n + r_2 \\ &\vdots \\ bc_m &= q_m n + r_m, \end{aligned}$$

where each remainder r_i satisfies $0 \leq r_i < n$. We first show that the remainders are all different. For suppose, by way of contradiction, that $r_i = r_j$ but $c_i \neq c_j$. Then we obtain

$$bc_i - q_i n = bc_j - q_j n.$$

This implies that n divides $b(c_i - c_j)$ However, as b and n are relatively prime, we deduce from Theorem 2.10 that n divides $c_i - c_j$. Now we are assuming that c_i is different from c_j and it then does no harm to assume that $c_i > c_j$. As n divides $c_i - c_j$, we obtain $c_i - c_j = rn$ for some positive integer r (since $c_i - c_j$ is positive). Hence $c_i = c_j + rn$. This means that, as c_j is positive, c_i is greater than n, contrary to the way in which these numbers were chosen. Thus we really do have $r_i \neq r_j$. Next we show that each r_i is relatively prime to n. For suppose that $\gcd(r_i, n) = d$ is greater than 1. Then there is a prime p, say that divides r_i and n. Since $bc_i = q_i n + r_i$, we deduce that p divides bc_i. Since p is a prime, Theorem 2.14 implies that p divides b or c_i. In the first case, p is a common divisor of b and n, in the second p is a common divisor of c_i and n, both of which are contrary to hypothesis. Thus we have $m = \varphi(n)$ different integers between 0 and $n-1$ which are all relatively prime to n. These can only be the c_i's in some order. ■

We move on now to prove Euler's generalization of Fermat's Little Theorem.

<u>(3.11) Theorem</u> Let $n > 1$ be an integer and let b be any integer relatively prime to n. Let $\varphi(n)$ denote the number of integers lying between 1 and n that are relatively prime to n. Then we have

$$b^{\varphi(n)} \equiv 1 \bmod n.$$

<u>Proof</u> As before, write $m = \varphi(n)$. Let $c_1, c_2, \ldots, c_m$ denote all the integers lying between 1 and n that are relatively prime to n, and let $r_1, \ldots, r_m$ be the remainders when $bc_1, \ldots, bc_m$ are divided by n. Lemma 3.10 implies that

$$r_1 r_2 \cdots r_m = c_1 c_2 \cdots c_m.$$

However, $bc_i \equiv r_i \bmod n$ and thus repeated use of Theorem 3.2 (iii) shows that

$$\begin{aligned}(bc_1)(bc_2)\cdots(bc_m) &\equiv r_1 r_2 \cdots r_m \bmod n \\ &\equiv c_1 c_2 \cdots c_m \bmod n.\end{aligned}$$

Hence, rearranging

$$b^{\varphi(n)} c_1 c_2 \cdots c_m \equiv c_1 c_2 \cdots c_m \bmod n$$

leading to

$$(b^{\varphi(n)} - 1) c_1 c_2 \cdots c_m \equiv 0 \bmod n.$$

As each of $c_1, c_2, \ldots, c_m$ is relatively prime to n we deduce from Theorem 2.10 that

$$b^{\varphi(n)} - 1 \equiv 0 \bmod n$$

which proves what we want. ■

Observe that Euler's theorem generalizes Fermat's Little Theorem. For, if we take $n = p$, where p is a prime, the integers lying between 1 and p that are relatively prime to p are

$$1, 2, 3 \ldots, p - 1$$

and thus $\varphi(p) = p - 1$. Note also that in the approach given in Theorem 3.11 there is no need to investigate binomial coefficients.

Example

Take $n = 25$. The integers lying between 1 and 25 that are relatively prime to 25 are those not divisible by 5, and thus are

$$1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24$$

and thus we get $\varphi(25) = 20$. It follows that if b is relatively prime to 25 (hence not divisible by 5), we get

$$b^{20} \equiv 1 \bmod 25.$$

Next, we proceed to calculate $\varphi(n)$ in a systematic way for any value of n. We begin with the case that n is a power of a prime p.

(3.12) Lemma Let p be a prime and let r be a positive integer. Then we have

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

Proof Instead of calculating the number of integers between 1 and p^r that are relatively prime to p^r, we calculate the number for which the gcd is greater than 1. It is clear that an integer has a common factor with p^r precisely when p divides that integer. We therefore calculate the number of integers between 1 and p^r that are divisible by p. The integers in question are

$$1 \times p = p,\ 2 \times p = 2p, \ldots,\ p^{r-1} \times p = p^r$$

and hence there are p^{r-1} of them. As there are p^r integers between 1 and p^r and for p^{r-1} the gcd with p^r is greater than 1,

$$p^r - p^{r-1} = p^{r-1}(p-1)$$

are relatively prime to p^r. ■

We prove next a simple fact relating to the gcd of a product of integers.

<u>(3.13) Lemma</u> Let m and n be integers. Then an integer r is relatively prime to mn if and only if it is relatively prime to both m and n.

<u>Proof</u> Consider first an integer r that is relatively prime to mn. Then we claim that r is relatively prime to both m and n. For if $d = \gcd(r, m)$, then d divides both r and m and hence divides r and mn. Thus d is a common divisor of r and mn and thus must be 1, since $\gcd(r, mn) = 1$ by assumption. Similarly, $\gcd(r, n) = 1$. Conversely, suppose that s is an integer relatively prime to both m and n and let $e = \gcd(s, mn)$. We claim that $e = 1$. For if this is not true, e is divisible by some prime p. Then p divides s and also mn. By Theorem 2.14, p divides one of m and n, say m. But then p is a common divisor s and m, contrary to the assumption that $\gcd(s, m) = 1$. Hence $e = 1$, as required. ■

In order to make use of Lemma 3.12, we need the following important fact.

<u>(3.14) Theorem</u> Let m and n be relatively prime positive integers. Then we have

$$\varphi(mn) = \varphi(m)\varphi(n).$$

<u>Proof</u> We calculate the number of integers lying between 1 and mn that are relatively prime to both m and n. By Lemma 3.13 above, this equals the number of integers between 1 and mn relatively prime to mn, which is what we want to find. We write down all the integers between 1 and mn according to the following scheme

$$\begin{array}{ccccc}
1 & 1+m & 1+2m & \ldots & 1+(n-1)m \\
2 & 2+m & 2+2m & \ldots & 2+(n-1)m \\
3 & 3+m & 3+2m & \ldots & 3+(n-1)m \\
\vdots & \vdots & \vdots & & \vdots \\
r & r+m & r+2m & \ldots & r+(n-1)m \\
\vdots & \vdots & \vdots & & \vdots \\
m & 2m & 3m & \ldots & nm
\end{array}$$

We want to look for integers in this scheme that are relatively prime to both m and n. Let r be a positive integer not exceeding m. If $d = \gcd(m, r)$ is bigger than 1, clearly no integer in the r-th row is relatively prime to m, since all integers in this row are divisible by d. Thus, as we are certainly looking for integers in the scheme that are relatively prime to m, we need only look in the r-th row, where $\gcd(m, r) = 1$. So, take such an integer r with $\gcd(r, m) = 1$. The integers in the r-th row are

$$r,\ r + m,\ r + 2m, \ldots,\ r + (n - 1)m$$

and we claim that they are all relatively prime to m. For consider a typical integer $r + km$ in this row and let $e = \gcd(m, r + km)$. Then e divides m and hence km, and therefore e divides $r + km - km = r$, since e also divides $r + km$. Thus e is a common divisor of m and r, which implies that $e = 1$, since $\gcd(r, m) = 1$.

We show next that no two of these n integers in the r-th row are congruent modulo n. For suppose we have

$$r + im \equiv r + jm \bmod n,$$

where $0 \leq i \leq n - 1$, $0 \leq j \leq n - 1$. Then we obtain that

$$n \text{ divides } im - jm = (i - j)m.$$

But as $\gcd(m, n) = 1$, Theorem 2.11 implies that n divides $i - j$ and this is only possible if $i - j = 0$. This proves what we want.

Our argument has shown that the n integers

$$r,\ r + m,\ r + 2m, \ldots,\ r + (n - 1)m$$

give rise to n different remainders modulo n (these remainders being 0, 1, 2, $\ldots$, $n - 1$ in some order). Consequently, exactly $\varphi(n)$ of the integers in the r-th row are relatively prime to n, since this is true of their remainders modulo n. We have $\varphi(m)$ choices for r and $\varphi(n)$ integers relatively prime to n in each row for each choice of r, giving

$$\varphi(m)\varphi(n)$$

integers that are relatively prime to both m and n and hence to mn. This implies that

$$\varphi(mn) = \varphi(m)\varphi(n)$$

and completes the proof. ■

We can now evaluate $\varphi(n)$ in general.

<u>(3.15) Theorem</u> Let n be a positive integer and let $p_1, \ldots, p_r$ be all the different prime divisors of n. Let

$$n = p_1^{a_1} \cdots p_r^{a_r}$$

be the factorization of n into primes. Then

$$\begin{aligned}\varphi(n) &= p_1^{a_1-1}(p_1-1)\cdots p_r^{a_r-1}(p_r-1)\\ &= n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_r}).\end{aligned}$$

<u>Proof</u> As the integers $p_1^{a_1}$, $p_2^{a_2} \cdots p_r^{a_r}$ are relatively prime to each other, Theorem 3.14 and Lemma 3.12 show that

$$\varphi(n) = \varphi(p_1^{a_1})\varphi(p_2^{a_2}\cdots p_r^{a_r}) = p_1^{a_1-1}(p_1-1)\varphi(p_2^{a_2}\cdots p_r^{a_r}).$$

Repetition of the argument leads to the desired conclusion. ■

<u>Example</u>

Evaluate $\varphi(210)$. Here,

$$210 = 2 \times 3 \times 5 \times 7$$

and thus

$$\begin{aligned}\varphi(210) &= \varphi(2)\varphi(3)\varphi(5)\varphi(7)\\ &= (2-1)(3-1)(5-1)(7-1) = 48.\end{aligned}$$

This shows that there are 48 integers between 1 and 210 that are relatively prime to 210 and hence not divisible by any of 2, 3, 5 or 7. With the exception of 1, such integers are either primes or are non-primes that are products of primes drawn from 11 and 19. The only such numbers are $11^2 = 121$, $13^2 = 169$ and $11 \times 13 = 143$, $11 \times 17 = 187$ and $11 \times 19 = 209$ Thus there are $48 - 6 = 42$ primes between 1 and 210 different from 2, 3, 5 and 7, hence 46 primes between 1 and 210.

<u>Example</u>

Find the smallest positive integer a so that

$$11^{100} \equiv a \bmod 45.$$

Now $45 = 3^2 \times 5$ and thus

$$\varphi(45) = 6 \times 4 = 24.$$

Since 11 and 45 are relatively prime, Euler's theorem implies that

$$11^{24} \equiv 1 \bmod 45.$$

Hence

$$11^{24\times 4} \equiv 1 \bmod 45.$$

Thus

$$11^{100} = 11^{96}11^4 \equiv 11^4 \bmod 45.$$

But $11^2 = 121 \equiv -14 \bmod 45$ and thus $11^4 \equiv 196 \equiv 16 \bmod 45$. It follows that $a = 16$.

We move on to consider a more complicated congruence problem. We need some preliminary lemmas.

<ins>(3.16) Lemma</ins> Let a be a non-zero integer and let $m_1, \ldots, m_n$ be integers with

$$\gcd(a, m_1) = \cdots = \gcd(a, m_n) = 1$$

(so that a is relatively prime to each of the m_i). Then a is relatively prime to $m_1 \cdots m_n$.

<ins>Proof</ins> Suppose that the two integers are not relatively prime. Then there exists a prime p that divides a and $m_1 \cdots m_n$. But then p divides some m_i, by Theorem 2.14. Such a p is a common divisor of a and m_i, contrary to hypothesis. Thus the two integers are relatively prime. ■

<ins>(3.17) Lemma</ins> Let $m_1, \ldots, m_n$ be integers that are pairwise relatively prime (so that $\gcd(m_i, m_j) = 1$ if $i \neq j$) and suppose that each m_i divides some integer c. Then the product $m_1 \cdots m_n$ divides c.

Proof We proceed by induction on n. The result is true for $n = 1$. Suppose the result is true when $n = r$. Then $m_1 \cdots m_r$ divides c. Now we wish to prove the result when $n = r + 1$. By Lemma 3.16, m_{r+1} is relatively prime to $m_1 \cdots m_r$ and thus there exist integers s and t with

$$sm_{r+1} + t(m_1 \cdots m_r) = 1.$$

Hence multiplying by c, we get

$$sm_{r+1}c + t(m_1 \cdots m_r)c = c.$$

Since both m_{r+1} and $m_1 \cdots m_r$ divide c, we have

$$c = m_{r+1}e, \quad c = (m_1 \cdots m_r)f,$$

for certain integers e and f. Substituting these values for c into our earlier equation, we obtain

$$m_{r+1}(m_1 \cdots m_r)sf + m_{r+1}(m_1 \cdots m_r)te = m_1 \cdots m_r m_{r+1}(sf + te) = c$$

which shows that $m_1 \cdots m_{r+1}$ divides c. This completes the induction step and proves the theorem. ■

Now we can prove our congruence theorem, known as the Chinese remainder theorem, as it is found in ancient Chinese mathematical manuscripts.

(3.18) Theorem (Chinese remainder theorem) Let $m_1, \ldots, m_n$ be positive integers that are pairwise relatively prime (so that $\gcd(m_i, m_j) = 1$ if $i \neq j$). Let $a_1, \ldots, a_n$ be any integers. Then there exists an integer solution x to the following system of congruences:

$$\begin{array}{ccc} x & \equiv & a_1 \bmod m_1 \\ x & \equiv & a_2 \bmod m_2 \\ \vdots & \vdots & \vdots \\ x & \equiv & a_n \bmod m_n. \end{array}$$

If x' is any other solution, then we have $x \equiv x' \bmod m_1 m_2 \cdots m_n$. There is a unique solution lying between 1 and $m_1 m_2 \cdots m_n$.

Proof Pick any index i lying between 1 and n. We first show that there is an integer x_i satisfying

$$\begin{array}{ccc} x_i & \equiv & 0 \bmod m_1 \\ \vdots & \vdots & \vdots \\ x_i & \equiv & 0 \bmod m_{i-1} \\ x_i & \equiv & 1 \bmod m_i \\ x_i & \equiv & 0 \bmod m_{i+1} \\ \vdots & \vdots & \vdots \\ x_i & \equiv & 0 \bmod m_n. \end{array}$$

We set $k_i = (m_1 \cdots m_n)/m_i$. By Lemma 3.16, m_i is relatively prime to k_i. Hence there exist integers r_i and s_i with

$$r_i k_i + s_i m_i = 1.$$

Therefore, we obtain

$$r_i k_i \equiv 0 \bmod k_i$$

$$r_i k_i \equiv 1 \bmod m_i.$$

But $m_1, \ldots, m_{i-1}, m_{i+1}, \ldots, m_n$ all divide k_i. Hence, if we set $x_i = r_i k_i$, we clearly have

$$\begin{array}{ccc} x_i & \equiv & 0 \bmod m_1 \\ \vdots & \vdots & \vdots \\ x_i & \equiv & 0 \bmod m_{i-1} \\ x_i & \equiv & 1 \bmod m_i \\ x_i & \equiv & 0 \bmod m_{i+1} \\ \vdots & \vdots & \vdots \\ x_i & \equiv & 0 \bmod m_n, \end{array}$$

as required. Finally, to solve the original congruence, we set

$$x = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n.$$

From the previous congruences, it is easy to see that

$$x \equiv a_i x_i \bmod m_i$$

and hence

$$x \equiv a_i \bmod m_i,$$

since $x_i \equiv 1 \bmod m_i$. Thus this x value solves the congruences. If we take the remainder r on the division of x by $m_1 \cdots m_n$, we claim that r also satisfies the congruence.

For since $x \equiv r \bmod m_1 \cdots m_n$, it is clear that $x \equiv r \bmod m_i$ for each i and thus $r \equiv a_i \bmod m_i$ for each i, as required.

To investigate other solutions, suppose that x' also solves the congruences. Then we have

$$x \equiv x' \equiv a_i \bmod m_i$$

for all i and hence

$$x - x' \equiv 0 \bmod m_i$$

for all i. As the m_i are pairwise relatively prime, Lemma 3.17 implies that $m_1 \cdots m_n$ divides $x - x'$, so that

$$x - x' \equiv 0 \bmod m_1 \cdots m_n,$$

as required. The solution described above is thus the unique one between 1 and $m_1 \cdots m_n$. ■

Example Find an integer solution x of the congruences

$$x \equiv 7 \bmod 11$$

$$x \equiv 3 \bmod 18$$

$$x \equiv 7 \bmod 25,$$

where x is an integer between 1 and $11 \times 18 \times 25 = 4950$.

We start by finding x_1 with

$$x_1 \equiv 1 \bmod 11$$

$$x_1 \equiv 0 \bmod 18$$

$$x_1 \equiv 0 \bmod 25.$$

Following the proof, we set $k_1 = 18 \times 25 = 450$. We try to find integers r_1 and s_1 with

$$450 r_1 + 11 s_1 = 1.$$

Following the Euclidean algorithm, we get $r_1 = -1$, $s_1 = 41$. Then according to the proof $x_1 = 450 r_1 = -450$.

Now we look for x_2 with

$$x_2 \equiv 0 \bmod 11$$

$$x_2 \equiv 1 \bmod 18$$

$$x_2 \equiv 0 \bmod 25.$$

We set $k_2 = 11 \times 25 = 275$ and look for r_2 and s_2 with

$$275r_2 + 18s_2 = 1.$$

By the Euclidean algorithm, we find $r_2 = -7$ and $s_2 = 107$. Hence we take $x_2 = 275r_2 = -1925$. Finally look for x_3 with

$$x_3 \equiv 0 \bmod 11$$

$$x_3 \equiv 0 \bmod 18$$

$$x_3 \equiv 1 \bmod 25.$$

We take $k_3 = 11 \times 18 = 198$ and look for r_3 and s_3 so that

$$198r_3 + 25s_3 = 1.$$

We obtain $r_3 = 12$ and $s_3 = -95$. Hence $x_3 = 198r_3 = 2376$. The solution for x is

$$-450 \times 7 - 1925 \times 3 + 7 \times 2376 = 7707.$$

Calculating the remainder when 7707 is divided by 4950, we reach the solution 2757, which is the unique one in the given range. To check, we have

$$2757 \equiv 7 \bmod 11 \text{ as } 11 \text{ divides } 2750$$

$$2757 \equiv 3 \bmod 18 \text{ as } 18 \text{ divides } 2754$$

$$2757 \equiv 7 \bmod 25 \text{ as } 25 \text{ divides } 2750$$

2757 is the unique solution in the specified range.