Introduction to modular arithmetic S2

Our discussions lie always in the set of integers ($\mathbb{Z}$).

GCD and HCF

The *greatest common divisor (GCD)* or *highest common factor (HCF)* is the greatest or highest number (integer) that will divide a given set of numbers.

What is the gcd of the numbers (60,84,210)?

Look at the gcd of just 60, 84 at first.

Guessing: 2 as 2|60 and 2|84 (| denotes divides). 60=2.30, 84=2.42. Again 2 divides both 30 and 42, 30=2.15, 42=2.21. Thus far $60 = 2^2.15$, $84 = 2^2.21$.

Now 3|15 and 3|21 i.e., 15=3.5, 21=3.7. We now have $60 = 2^2.3.5$, $84 = 2^2.3.7$.

Numbers 5 and 7 have no common factor other than 1. We conclude gcd(60,84)= $2^2.3 = 12$. 60=12.5 and 84=12.7.

Now find the gcd of 12 and 210. Factoring 210 we get 210=3.70=3.7.10=3.7.2.5.

Then see that the gcd(60,84,210)=gcd(12,210)=gcd(2,2,3 and 2.3.5.7) =2.3=6.

Often one omits the abbreviation gcd and just writes (60,84)=12 or (60,84,210)=6.

Euclid's algorithm for finding the gcd

Divide 84 by 60 which has remainder, thus $84 = 1.60 + 24$

Divide the divisor (60) by the remainder (24) to get $60 = 2.24 + 12$

Divide the divisor (24) by the remainder (12) to get $24 = 2.12$ with no remainder.

So 12 is the gcd of 60 and 84.

Continue on with 210 and 12, so that $210 = 17.12 + 6$

Next line $12 = 2.6$ with no remainder.

So finally gcd(60,84,210) = 6.

Given two numbers a,b if gcd(a,b) = 1, that is, they have no factor in common other than unity, we say that they are *relatively prime*, or *coprime*. If a set of numbers have gcd=1 we say that they are each *relatively prime in pairs* or *coprime* to every other in the set.

Exercise 2

Find the gcd of 78,696 and 19,332 using Euclid's algorithm.

Fundamental Theorem of Arithmetic - (some 'large numbers!)

Every number can be written as a product of prime power factors. For example $4410 = 2.3^2.5.7^2$.

Can you factorize

$$\begin{aligned} N \quad = \quad & 114,381,625,757,888,867,669,235,779,976,146,612,010,218,296, \\ & 721,242,362,562,561,842,935,706,935,245,733,897,830,597,123, \\ & 563,958,705,058,989,075,147,599,290,026,879,543,541 \end{aligned}$$

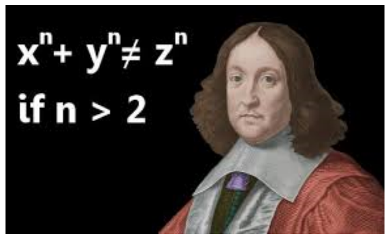
This very large number (129 digits) is a product of two very large prime numbers.

A *googol* is 1 with a hundred zeros after it

$$\begin{aligned} G &= 10,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,\\ &\quad 000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000 \\ &= 10^{100} \end{aligned}$$

A *googolplex* is 10^{googol}.

Pierre de Fermat



c 1607 - 1685

Isaac Newton - 1643-1727. Fermat was 36 when Newton was born.

Fermat was the first person known to have evaluated the integral of general power functions. With his method, he was able to reduce this evaluation to the sum of geometric series. The resulting formula was helpful to Newton, and then Leibniz, when they independently developed the fundamental theorem of calculus.

In number theory, Fermat studied Pell's equation, perfect numbers, amicable numbers and what would later become Fermat numbers. It was while researching perfect numbers that he discovered Fermat's little theorem. He invented a factorization method—Fermat's factorization method—as well as the proof technique of infinite descent, which he used to prove Fermat's right triangle theorem which includes as a corollary Fermat's Last Theorem for the case n = 4. Fermat developed the two-square theorem, and the polygonal number theorem, which states that each number is a sum of three triangular numbers, four square numbers, five pentagonal numbers, and so on.

Although Fermat claimed to have proven all his arithmetic theorems, few records of his proofs have survived. Many mathematicians, including Gauss, doubted several of his claims, especially given the difficulty of some of the problems and the limited mathematical methods available to Fermat.

His famous Last Theorem was first discovered by his son in the margin in his father's copy of an edition of Diophantus, and included the statement that the margin was too small to include the proof. It seems that he had not written to Marin Mersenne about it. It was first proven in 1994, by Sir Andrew Wiles, using techniques unavailable to Fermat.

Although Pythagoras Theorem $x^2 + y^2 = z^2$ has integer solutions, the equation $x^n + y^n = z^n$ for $n > 2$ has no +ve integer solutions (Fermat's Last Theorem).

The full text of Fermat's statement, written in Latin, reads "Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet" (Nagell 1951, p. 252). In translation,

"*It is impossible for a cube to be the sum of two cubes, a fourth power to be the sum of two fourth powers, or in general for any number that is a power greater than the second to be the sum of two like powers.*

I have discovered a truly marvelous demonstration of this proposition that this margin is too narrow to contain."

A *polynomial*, or *polynomial expression*, in a variable, is a sum of terms in powers of the variable - with each power multiplied by a coefficient. Thus a polynomial, of degree n in x is of the form

$$f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n$$

We have seen that, if

$$x \equiv y(\mathrm{mod}\, m)$$

then

$$\begin{array}{ll} x \equiv y(\mathrm{mod}\, m) & a_{n-1}x \equiv a_{n-1}y(\mathrm{mod}\, m) \\ x^2 \equiv y^2(\mathrm{mod}\, m) & a_{n-2}x^2 \equiv a_{n-2}y^2(\mathrm{mod}\, m) \\ \cdot \quad \cdot \quad \cdot & \cdot \quad \cdot \quad \cdot \\ x^n \equiv y^n(\mathrm{mod}\, m) & a_0x^n \equiv a_0y^n(\mathrm{mod}\, m) \end{array}$$

That is

$$f(x) \equiv f(y)(\mathrm{mod}\, m)$$

A *polynomial equation* is of the form $f(x) = 0$.

Fermat numbers (1607-1665 French lawyer and mathematician)

Fermat stated, though confessing he did not posess a valid proof, that all numbers of the form

$$2^{2^n} + 1$$

are primes.This statement was refuted by Euler, who showed that the number $2^{2^5} = 2^{32}$ was divisible by 641.

Without calculating 2^{32} explicitly, the divisibility of this large number by 641 can be established with the help of congruences fairly easily.

We have (mod 641 in operation)

$$\begin{array}{rcl} 2^2 & \equiv & 4, \qquad 2^4 \equiv 16 \qquad 2^8 \equiv 256 \qquad 2^{16} = 256^2 \equiv 154(\mathrm{mod}\, 641) \\ 2^{32} & \equiv & 154^2 \equiv 640(\mathrm{mod}\, 641) \qquad \text{so } 2^{32} + 1 \equiv 641 \equiv 0(\mathrm{mod}\, 641). \end{array}$$

The numbers $F_n = 2^{2^n} + 1$ are called *Fermat numbers.*

As of 2016, the only known Fermat primes are $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$.

$F_{11} = 2^{2^{11}} + 1 = 32{,}317{,}006{,}071{,}311{,}007{,}300{,}714{,}8...193{,}555{,}853{,}611{,}059{,}596{,}230{,}657$ (617 digits)

$= 319{,}489 \times 974{,}849 \times 167{,}988{,}556{,}341{,}760{,}475{,}137(21 digits) \times 3{,}560{,}841{,}906{,}445{,}833{,}920{,}513(22 digits) \times$ 173,462,447,179,147,555,430,258...491,382,441,723,306,598,834,177 (564 digits) (fully factored 1988)

There are no other known Fermat primes F_n with $n > 4$. However, little is known about Fermat numbers with large n. In fact, each of the following is an open problem:

Is F_n composite for all n > 4?

Are there infinitely many Fermat primes? (Eisenstein 1844)

Are there infinitely many composite Fermat numbers?

Does a Fermat number exist that is not square-free?

As of 2014, it is known that F_n is composite for $5 \leq n \leq 32$, although amongst these, complete factorizations of F_n are known only for $0 \leq n \leq 11$, and there are no known prime factors for n = 20 and n = 24. The largest Fermat number known to be composite is $F_{3329780}$, and its prime factor $193 \times 2^{23329782} + 1$, a megaprime, was discovered by the PrimeGrid collaboration in July 2014.

Mersenne numbers (Mersenne 1588-1648, an ordained priest and polymath)

A number of the form $M_p = 2^p - 1$ where p is a prime number is called a *Mersenne number*. Such a number which is itself prime is also called a *Mersenne prime*.

A new Mersenne prime was found in December 2017. As of January 2018, 50 are now known. The largest known prime number $M_{77,232,917} = 2^{77,232,917} - 1$ is a Mersenne prime with 23,249,425 digits. It was found by the Great Internet Mersenne Prime Search (GIMPS) in 2017.Since 1997, all newly found Mersenne primes have been discovered by the Great Internet Mersenne Prime Search (GIMPS), a distributed computing project on the Internet.

Example 1

Find the remainder obtained by dividing 3^{100} by 101.

In all cases when the exponent is large the operation will be greatly shortened by resorting to the fact that every integer is a sum of powers of 2. Thus in our case

$$100 = 64 + 32 + 4$$

and

$$3^{100} = 3^{64}.3^{32}.3^4.$$

Now assuming we are working (mod 101), but not writing it out every time we write, in short

$3^4 = 81 \equiv -20 \qquad 3^8 \equiv 20^2 \equiv -4 \qquad 3^{16} \equiv 16 \qquad 3^{32} \equiv 256 \equiv -47 \qquad 3^{64} \equiv 47^2 \equiv -13 (\mathrm{mod}\, 101)$

and again, $3^4.3^{32} \equiv (-20).(-47) \equiv 31$ and $3^4.3^{32}.3^{64} \equiv 31.(-13) = -403 \equiv 1 (\mathrm{mod}\, 101)$, that is

$$3^{100} \equiv 1 (\mathrm{mod}\, 101).$$

It is also true that, e.g., $28^{100} \equiv 1 (\mathrm{mod}\, 101)$ or $85^{100} \equiv 1 (\mathrm{mod}\, 101)$ or indeed any number a (not a muliple of 101) satisfies

$$a^{100} \equiv 1 (\mathrm{mod}\, 101).$$

Or also $a^{72} \equiv 1 (\mathrm{mod}\, 73)$ for any a not a multiple of 73, or $a^{3670} \equiv 1 (\mathrm{mod}\, 3671)$ etc., etc.

What is noticeable about these congruences?

Example 2

Familiar criteria of divisibility by $3, 9, 11$ follow immediately from the properties of congruences. Let a number N be represented in the decimal notation thus:

$$N = a + 10b + 10^2c + 10^3d + \cdots$$

Noticing that

$$10 \equiv 1 \qquad 10^2 \equiv 1 \qquad 10^3 \equiv 1, \qquad \ldots (\mathrm{mod}\, 9)$$

we have

$$N \equiv a + b + c + d + \cdots (\mathrm{mod}\, 9).$$

Hence a number is divisible by 9 if and only if the sum of its digits is divisible by 9. Since the congruence holding for a certain modulus evidently holds for any divisor of this modulus, we also have

$$N \equiv a + b + c + d + \cdots (\mathrm{mod}\, 3).$$

With respect to the modulus 11, we have

$$10 \equiv -1 \qquad 10^2 \equiv 1 \qquad 10^3 \equiv -1, \qquad \ldots (\mathrm{mod}\, 11)$$

and so

$$N \equiv a - b + c - d + \cdots (\mathrm{mod}\, 11)$$

Euler's ϕ function or totient

If m is a +ve integer the number of +ve integers less than m and relatively prime to m is denoted by $\phi(m)$ and ϕ is called *Euler's totient or ϕ function.* (The number 1 is counted).

For example, if $m = 12$, $\phi(12) = \{\} = 4$.

If p is prime, $\phi(p) = p - 1$. More generally, $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$. If $\alpha = 1$ this says $\phi(p) = p - 1$.

Euler's totient is useful in cryptography.

Let the integer n be expressed as the product of its prime powers

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} \qquad \text{think of } 360 = 2^3.3^2.5$$

Then

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_s})$$

If n is a power of a single prime, say $n = p^\alpha$ then

$$\phi(p^\alpha) = p^\alpha(1 - \frac{1}{p}) = p^\alpha - p^{\alpha-1} \qquad \text{see above.}$$

For $n = 360$, we get $\phi(360) = 360(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 360.\frac{1}{2}.\frac{2}{3}.\frac{4}{5} = 96$ - is the number of +ve integers less than 360 and relatively prime to it.

Euler's Theorem

If a is relatively prime to m then

$$a^{\phi(m)} \equiv 1 (\mathrm{mod}\, m).$$

So, for $m = 360$, where $\phi(m) = 96$ we have, for any integer a relatively prime to 360, that is, $(a, 360) = 1$ we have

$$a^{96} \equiv 1 (\mathrm{mod}\, 360).$$

Most particularly if $m = p$ a prime, so that $\phi(p) = p - 1$ - see above - we get for any integer a such that $(a, p) = 1$,

Fermat's Little Theorem

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p)$$

Thus for example

$$3^{100} \equiv 1(\mathrm{mod}\, 101) \qquad \text{and} \qquad 94^{72} \equiv 1(\mathrm{mod}\, 73) \qquad \text{and} \qquad 1000000^{3670} \equiv 1(\mathrm{mod}\, 3671)$$

Bezout's Theorem - Many congruences

If $x \equiv a(\mathrm{mod}\, m_1)$ and $x \equiv b(\mathrm{mod}\, m_2)$ then there exist integers p_1, p_2 such that

$$m_1 p_1 + m_2 p_2 = \gcd(a, b).$$

A solution, now of both congruences is

$$x = b m_1 p_1 + a m_2 p_2$$

That is

$$x \equiv b m_1 p_1 + a m_2 p_2 (\mathrm{mod}\, m_1 m_2).$$

Example 3

Solve the congruences

$$\begin{aligned} x &\equiv 2(\mathrm{mod}\, 3) \\ x &\equiv 3(\mathrm{mod}\, 5) \\ x &\equiv 2(\mathrm{mod}\, 7). \end{aligned}$$

Consider just the first two congruences. Here, $m_1 = 3, m_2 = 5, m_3 = 7$. And $a = 2, b = 3$, and we put $c = 2$ for the third congruence.

Then, x will be congruent to $3.5.7 = 105$.

For the first two congruences $\gcd(3, 5) = 1$. Can we find integers p_1 and p_2 such that

$$3p_1 + 5p_2 = 1$$

This can be solved as a congruence, but a mental solution quickly appears as $p_1 = 2$, $p_2 = -1$.

Thus a solution of the first two congruences is

$$x = 3.3.2 + 2.5.(-1) = 8.$$

So far we then have

$$x \equiv 8(\mathrm{mod}\, 3.5) \equiv 8(\mathrm{mod}\, 15).$$

So any x that satisfies this latter congruence also satisfies both the first and second congruences, e.g., 23, -7, 68 etc.

Now use this with the third congruence, that is

$$\begin{aligned} x &\equiv 8(\mathrm{mod}\, 15) \\ x &\equiv 2(\mathrm{mod}\, 7) \end{aligned}$$

(Can we 'guess' a solution? Try using some numbers that solve the first congruence!)

Otherwise - GOOD EXERCISE - solve the two congruences by the method used above! You should get

$$\begin{aligned} x &\equiv 23 (\mathrm{mod}\, 105) \text{ or} \\ x &= 23 + 105k \text{ where } k \text{ is an integer} \end{aligned}$$

CHECK. See the image on the rhs in the Wikipedia article
https://en.wikipedia.org/wiki/Chinese_remainder_theorem.

From Wiki: The earliest known statement of the theorem, as a problem with specific numbers, appears in the 3rd-century book Sunzi Suanjing by the Chinese mathematician Sunzi.

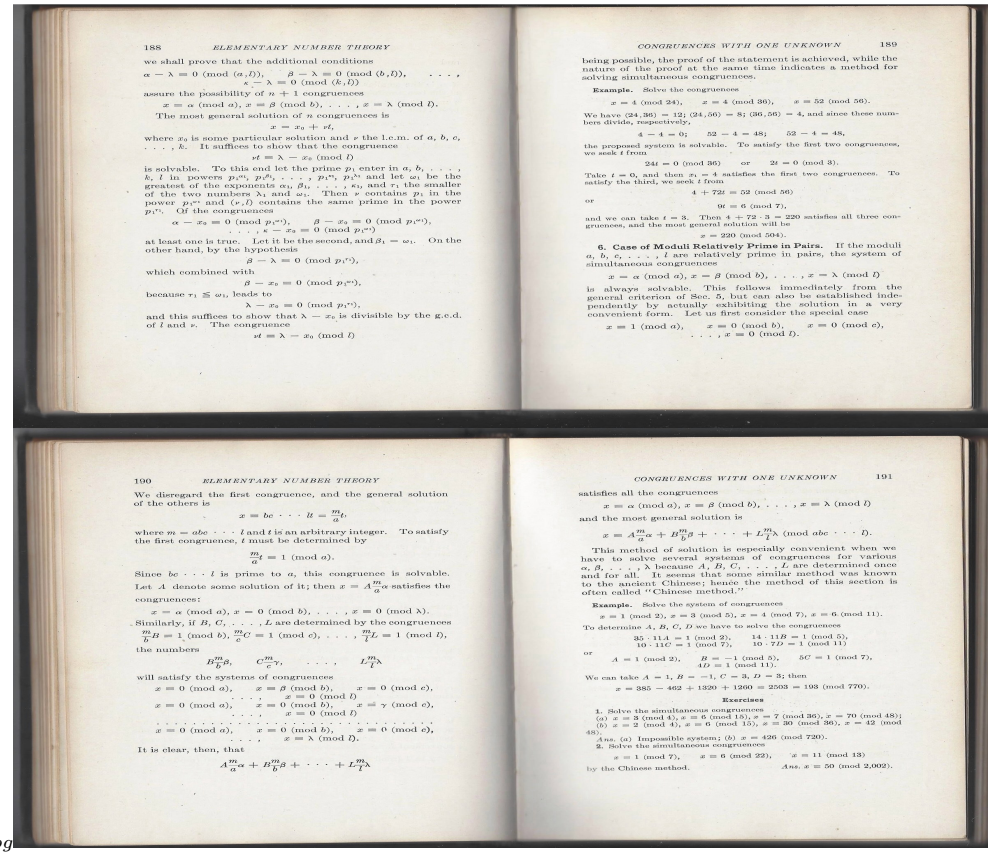
Sunzi's work contains neither a proof nor a full algorithm. What amounts to an algorithm for solving this problem was described by Aryabhata (6th century). Special cases of the Chinese remainder theorem were also known to Brahmagupta (7th century), and appear in Fibonacci's *Liber Abaci* (1202). The result was later generalized with a complete solution called Dayanshu in Qin Jiushao's 1247 Mathematical Treatise in Nine Sections (Shushu Jiuzhang).

Chinese Remainder Theorem
https://www.youtube.com/watch?v=3PkxN_r9up8
https://www.youtube.com/watch?v=3PkxN_r9up8
Read s 6. Case of Moduli relatively prime in pairs.
Read, particularly, the Example.

Remainder

Theorem

Chinese remainder Theorem
https://www.youtube.com/watch?v=3PlxN_r9up8 https://www.youtube.com/watch?v=3PlxN_r9up8
Read s 6. Case of Moduli relatively prime in pairs.
Read, particularly, the Example.



188 ELEMENTARY NUMBER THEORY

we shall prove that the additional conditions

$$\alpha - \lambda = 0 \pmod{(a,b)}, \quad \beta - \lambda = 0 \pmod{(b,c)}, \quad \cdots, \quad \kappa - \lambda = 0 \pmod{(k,l)}$$

assure the possibility of $n+1$ congruences

$$x = \alpha \pmod{a}, \; x = \beta \pmod{b}, \; \cdots, \; x = \lambda \pmod{l}.$$

The most general solution of n congruences is

$$x = x_0 + \nu t,$$

where x_0 is some particular solution and ν the l.c.m. of $a, b, c, \cdots, k$. It suffices to show that the congruence

$$\nu t = \lambda - x_0 \pmod{l}$$

is solvable. To this end let the prime p_1 enter in $a, b, \cdots, k, l$ in powers $p_1^{\alpha_1}, p_1^{\beta_1}, \cdots, p_1^{\kappa_1}, p_1^{\lambda_1}$ and let ω_1 be the greatest of the exponents $\alpha_1, \beta_1, \cdots, \kappa_1$ and r_1 the smaller of the two numbers λ_1 and ω_1. Then ν contains p_1 in the power $p_1^{\omega_1}$ and (ν, l) contains the same prime in the power $p_1^{r_1}$. Of the congruences

$$\alpha - x_0 = 0 \pmod{p_1^{\omega_1}}, \quad \beta - x_0 = 0 \pmod{p_1^{\omega_1}}, \quad \cdots, \quad \kappa - x_0 = 0 \pmod{p_1^{\omega_1}}$$

at least one is true. Let it be the second, and $\beta_1 = \omega_1$. On the other hand, by the hypothesis

$$\beta - \lambda = 0 \pmod{p_1^{r_1}},$$

which combined with

$$\beta - x_0 = 0 \pmod{p_1^{\omega_1}},$$

because $r_1 \leqq \omega_1$, leads to

$$\lambda - x_0 = 0 \pmod{p_1^{r_1}},$$

and this suffices to show that $\lambda - x_0$ is divisible by the g.c.d. of l and ν. The congruence

$$\nu t = \lambda - x_0 \pmod{l}$$

CONGRUENCES WITH ONE UNKNOWN 189

being possible, the proof of the statement is achieved, while the nature of the proof at the same time indicates a method for solving simultaneous congruences.

Example. Solve the congruences

$$x = 4 \pmod{24}, \quad x = 4 \pmod{36}, \quad x = 52 \pmod{56}.$$

We have $(24, 36) = 12$; $(24, 56) = 8$; $(36, 56) = 4$, and since these numbers divide, respectively,

$$4 - 4 = 0; \quad 52 - 4 = 48; \quad 52 - 4 = 48,$$

the proposed system is solvable. To satisfy the first two congruences, we seek t from

$$24t = 0 \pmod{36} \quad \text{or} \quad 2t = 0 \pmod{3}.$$

Take $t = 0$, and then $x_1 = 4$ satisfies the first two congruences. To satisfy the third, we seek t from

$$4 + 72t = 52 \pmod{56}$$

or

$$9t = 6 \pmod{7},$$

and we can take $t = 3$. Then $4 + 72 \cdot 3 = 220$ satisfies all three congruences, and the most general solution will be

$$x = 220 \pmod{504}.$$

6. Case of Moduli Relatively Prime in Pairs. If the moduli $a, b, c, \cdots, l$ are relatively prime in pairs, the system of simultaneous congruences

$$x = \alpha \pmod{a}, \; x = \beta \pmod{b}, \; \cdots, \; x = \lambda \pmod{l}$$

is always solvable. This follows immediately from the general criterion of Sec. 5, but can also be established independently by actually exhibiting the solution in a very convenient form. Let us first consider the special case

$$x = 1 \pmod{a}, \quad x = 0 \pmod{b}, \quad x = 0 \pmod{c}, \quad \cdots, \; x = 0 \pmod{l}.$$

190 ELEMENTARY NUMBER THEORY

We disregard the first congruence, and the general solution of the others is

$$x = bc \cdots lt = \frac{m}{a}t,$$

where $m = abc \cdots l$ and t is an arbitrary integer. To satisfy the first congruence, t must be determined by

$$\frac{m}{a}t = 1 \pmod{a}.$$

Since $bc \cdots l$ is prime to a, this congruence is solvable. Let A denote some solution of it; then $x = A\frac{m}{a}\alpha$ satisfies the congruences:

$$x = \alpha \pmod{a}, \; x = 0 \pmod{b}, \; \cdots, \; x = 0 \pmod{\lambda}.$$

Similarly, if $B, C, \cdots, L$ are determined by the congruences

$$\frac{m}{b}B = 1 \pmod{b}, \; \frac{m}{c}C = 1 \pmod{c}, \; \cdots, \; \frac{m}{l}L = 1 \pmod{l},$$

the numbers

$$B\frac{m}{b}\beta, \quad C\frac{m}{c}\gamma, \quad \cdots, \quad L\frac{m}{l}\lambda$$

will satisfy the systems of congruences

$$\begin{array}{lll} x = 0 \pmod{a}, & x = \beta \pmod{b}, & x = 0 \pmod{c}, \\ \cdots, & x = 0 \pmod{l} & \\ x = 0 \pmod{a}, & x = 0 \pmod{b}, & x = \gamma \pmod{c}, \\ \cdots, & x = 0 \pmod{l} & \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ x = 0 \pmod{a}, & x = 0 \pmod{b}, & x = 0 \pmod{c}, \\ \cdots, & x = \lambda \pmod{l}. & \end{array}$$

It is clear, then, that

$$A\frac{m}{a}\alpha + B\frac{m}{b}\beta + \cdots + L\frac{m}{l}\lambda$$

CONGRUENCES WITH ONE UNKNOWN 191

satisfies all the congruences

$$x = \alpha \pmod{a}, \; x = \beta \pmod{b}, \; \cdots, \; x = \lambda \pmod{l}$$

and the most general solution is

$$x = A\frac{m}{a}\alpha + B\frac{m}{b}\beta + \cdots + L\frac{m}{l}\lambda \pmod{abc \cdots l}.$$

This method of solution is especially convenient when we have to solve several systems of congruences for various $\alpha, \beta, \cdots, \lambda$ because $A, B, C, \cdots, L$ are determined once and for all. It seems that some similar method was known to the ancient Chinese; hence the method of this section is often called "Chinese method."

Example. Solve the system of congruences

$$x = 1 \pmod{2}, \; x = 3 \pmod{5}, \; x = 4 \pmod{7}, \; x = 6 \pmod{11}.$$

To determine A, B, C, D we have to solve the congruences

$$\begin{array}{ll} 35 \cdot 11A = 1 \pmod{2}, & 14 \cdot 11B = 1 \pmod{5}, \\ 10 \cdot 11C = 1 \pmod{7}, & 10 \cdot 7D = 1 \pmod{11} \end{array}$$

or

$$A = 1 \pmod{2}, \quad B = -1 \pmod{5}, \quad 5C = 1 \pmod{7}, \quad 4D = 1 \pmod{11}.$$

We can take $A = 1$, $B = -1$, $C = 3$, $D = 3$; then

$$x = 385 - 462 + 1320 + 1260 = 2503 = 193 \pmod{770}.$$

Exercises

1. Solve the simultaneous congruences
(a) $x = 3 \pmod{4}$, $x = 6 \pmod{15}$, $x = 7 \pmod{36}$, $x = 70 \pmod{48}$; (b) $x = 2 \pmod{4}$, $x = 6 \pmod{15}$, $x = 30 \pmod{36}$, $x = 42 \pmod{48}$.
Ans. (a) Impossible system; (b) $x = 426 \pmod{720}$.
2. Solve the simultaneous congruences

$$x = 1 \pmod{7}, \quad x = 6 \pmod{22}, \quad x = 11 \pmod{13}$$

by the Chinese method. *Ans.* $x = 50 \pmod{2,002}$.

2.jpg

You are doing very well indeed if you can follow the proof!!