Solving congruences

$\bar{a}$ is the inverse of a modulo m.

$\bar{a}$ might not exist

ex: Inverse of $3 \bmod 5 = 2$ (or 7) $(3 \cdot 2 \equiv 1 \bmod 5)$

Inverse of $2 \bmod 6$? doesn't exist

Solve for x

$ax \equiv b \bmod m$

want to find some number $\bar{a}$ such that $a\bar{a} \equiv 1 \bmod m$

so we would get

$1x \equiv a\bar{a} \equiv \bar{a} \cdot b \bmod m$

Theorem 1: If a and m are relatively prime then an inverse of $a \bmod m$ exists and is unique modulo m

Proof:

assuming a and m are relatively prime ($\gcd = 1$). Since $\gcd(a,m) = 1$ There exist some integers such that $s, t \in \mathbb{Z}$ such that $as + mt = 1$, so

$as \equiv 1 \bmod m$

Uniqueness: Exercise 7. To find the inverse of modulo m consider $a, 2a, 3a \ldots$ until you find one that is $1 \bmod m$

Example $3 \equiv 1 \bmod 7$ — $3, 6, 9, 12, 15$ (3·1, 3·2, 3·3, 3·4, 3·5) so 5 is the inverse of $3 \equiv 1 \bmod 7$

If $\gcd(a,m) \neq 1$, then there is no inverse of $a \bmod m$.

Example: Solve $3X \equiv 4 \bmod 7$

use stuff from before

multiply by inverse of $3 \equiv 1 \bmod 7$ is 5

$X \equiv 5 \cdot 4 \equiv 20 \equiv 6 \bmod 7$

Put 6 in for x, so $3 \cdot 6 = 18 \equiv 4 \bmod 7$ which is true

If it were $ax + b \equiv cx + d \bmod m$

move around: $ax - cx \equiv d - b \bmod m$

$(a-c)x \equiv d - b \bmod m$

Now there is a constant

So it can be solved

Chinese remainder theorem

solve a system of congruences

$x \equiv 2 \bmod 3$

$x \equiv 3 \bmod 5$

$x \equiv 5 \bmod 7$

Theorem: Let $m_1, m_2, \ldots, m_n$ be relatively prime positive integers, then the system has a unique system modulo $m = m_1 m_2 \ldots m_n$.

$x \equiv a_1 \bmod m_1$

$x \equiv a_2 \bmod m_2$

$x \equiv a_3 \bmod m_3$

$\vdots$

$x \equiv a_n \bmod m_n$

In other words, there is a solution $0 \leq x < m$ and all solutions are congruent to this one mod m

Proof: first prove the solution exists

$M_k = \frac{m}{m_k}$ for each $k = 1, 2, \ldots, n$

$\gcd(m_k, M_k) = 1$ since $\gcd(m_i, m_k) = 1$ for all $i \neq k$

because of there is an inverse y_k of m_k modulo M_k

i.e. $M_k y_k \equiv 1 \bmod m_k$

So $a_k \cdot M_k \cdot y_k \equiv a_k \bmod m_k$

Let $X = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_n M_n y_n$ — solution

Since $M_j \equiv 0 \bmod m_k$ for $j \neq k$

$M_j = \frac{m}{m_j} = \frac{m_1 m_2 \cdots m_n}{m_j} = m_1 m_2 \cdots m_{j-1} m_{j+1} \cdots m_n$

$a_j M_j y_j \equiv 0 \bmod k$ if $k \neq j$

$X \equiv a_1 M_1 y_1 + \ldots + a_n M_n y_n \equiv 0 + \ldots + 0 + a_k M_k y_k \equiv a_k \bmod m_k$

Prove uniqueness: suppose X and y are solutions to the systems. We must show $X \equiv y \bmod m$. Since $X \equiv y \bmod m_i$ for all $i = 1, \ldots, n$

By exercise 30 in the book $X \equiv y \bmod m$

Example $x \equiv 2 \bmod 3$, $x \equiv 3 \bmod 5$, $x \equiv 5 \bmod 7$

Check all moduli are relatively prime (these are)

$m = 3 \cdot 5 \cdot 7 = 105$

$M_1 = \frac{105}{3} = 35$ $\quad M_1 \equiv 35 \equiv 2 \bmod 3$ so $y_1 = 2$

$M_2 = \frac{105}{5} = 21$ $\quad M_2 \equiv 21 \equiv 1 \bmod 5$ so $y_2 = 1$

$M_3 = \frac{105}{7} = 15$ $\quad M_3 \equiv 15 \equiv 1 \bmod 7$ so $y_3 = 1$

Now we can compute x:

$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 5 \cdot 15 \cdot 1$

$= 140 + 63 + 75$

$= 278 \equiv 68 \bmod 105$

$x \equiv 68 \bmod 105$

Remember to make sure $y_n \equiv 1 \pmod{m_n}$

back substitution

Example

$x \equiv 1 \pmod 5$
$x \equiv 2 \pmod 6$
$x \equiv 3 \pmod 7$

take and put in other congruent

$x = 5t+1$
$5t+1 \equiv 2 \pmod 6$
$5t \equiv 1 \pmod 6$
$t \equiv 5 \pmod 6$
$t = 6u+5$ put into equation for x

$x = 5\cdot(6u+5)+1 = 30u+26$

$30u+26 \equiv 3 \pmod 7$
$2u-2 \equiv 3 \pmod 7$
$2u \equiv 5 \pmod 7$
$u \equiv 20 \equiv 6 \pmod 7$

$u = 7v+6$
$x = 30\cdot u+26 = 30\cdot(7v+6)+26 = 210v+206$

continue doing it until the final equation $x \equiv 206 \pmod{210}$

Fermat's little theorem

If p is a prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod p$
Moreover, for any integer a: $a^p \equiv a \pmod p$
Proof: exercise 19.

Example: Find $7^{222} \bmod 11$

$7^{222} = (7^{10})^{22}\cdot 7^2 \equiv 1^{22}\cdot 7^2 \equiv 1\cdot 49 \pmod{11} \equiv 5 \pmod{11}$

Use Fermat's little theorem: $7^{11-1} \equiv 1 \pmod{11}$

Def: let b be a positive integer. b and n must be relatively prime
If n is a composite positive integer and $b^{n-1} \equiv 1 \pmod n$, then n is called a pseudoprime to the base b.
Is a decent test to see if a number is a prime

455,052,512 primes $< 10^{10}$ there is 50 more primes less than 10^8
only 14884 pseudoprimes for base 2.

Def: a composite integer n that is a pseudoprime for all b such that $\gcd(b,n)=1$ is a Carmichael number

Ex: $561 = 3\cdot 11\cdot 17$
If $\gcd(b,561)=1$ then $\gcd(b,3)=\gcd(b,11)=\gcd(b,17)=1$

Using Fermat's little theorem:
$b^2 \equiv 1 \pmod 3$, $b^{10} \equiv 1 \pmod{11}$, $b^{16} \equiv 1 \pmod{17}$
$b^{560} = (b^2)^{280} \equiv 1 \pmod 3$
$b^{560} = (b^{10})^{56} \equiv 1 \pmod{11}$
$b^{560} = (b^{16})^{35} \equiv 1 \pmod{17}$

By exercise 29 $b^{560} \equiv 1 \pmod{561}$

Induction

Sometimes we want to prove statements $P(n)$ for all $n \in \mathbb{N}$

Example: $P(n)$ is the statement: $1+2+3+\dots+n = \frac{n\cdot(n+1)}{2}$ prove by induction

Two steps:
Basis step: Prove $P(1)$ is true
Inductive step: Prove that the statement "$P(n) \to P(n+1)$" is true for all $n \geq 1$

"$P(n)$ implies $P(n+1)$"

$P(1) = 1 = \frac{1(1+1)}{2}$ True $1 = \frac{2}{2}$

Inductive Step: Suppose $P(n)$ holds for some $n \in \mathbb{Z}^+$

$(1+2+\dots+n)+(n+1) = \frac{n\cdot(n+1)}{2}+(n+1)$
by assuming $P(n)$ holds, this is $\frac{n(n+1)}{2}$ so
$= \frac{n\cdot(n+1)+2(n+1)}{2} = \frac{(n+1)\cdot(n+2)}{2} = \frac{(n+1)\cdot((n+1)+1)}{2}$

Exercises

4.4: 5, 9, 11, 21, 24, 39, 47, 7, 19, 29, 35, 43, 53

5.1: 3, 5, 1, 7

5

a) $7 \cdot 4 \cdot 7 = 28 \cdot 28 \equiv 1 \pmod 9$

b) $52 \cdot 52 \cdot 17 = 988 \cdot 988 \equiv 1 \pmod{141}$

c) $34 \cdot 55 \cdot 34 = 1870 \cdot 1870 \equiv 1 \pmod{89}$

d) $a = 89, m = 232$

$232 = 2 \cdot 89 + 54$
$89 = 1 \cdot 54 + 35$
$54 = 1 \cdot 35 + 19$
$35 = 1 \cdot 19 + 16$
$19 = 1 \cdot 16 + 3$
$16 = 5 \cdot 3 + 1$
$3 = 3 \cdot 1 + 0$

$1 = 16 - 5 \cdot 3$
$= 16 - 5 \cdot (19 - 1 \cdot 16) = -5 \cdot 19 + 6 \cdot 16$
$= -5 \cdot 19 + 6 \cdot (35 - 1 \cdot 19) = 6 \cdot 35 - 11 \cdot 19$
$= 6 \cdot 35 - 11 \cdot (54 - 1 \cdot 35) = -11 \cdot 54 + 17 \cdot 35$
$= -11 \cdot 54 + 17 \cdot (89 - 1 \cdot 54) = 17 \cdot 89 - 28 \cdot 54$
$= 17 \cdot 89 - 28 \cdot (232 - 2 \cdot 89) = -28 \cdot 232 + 73 \cdot 89$

9

$x \equiv 7 \cdot 5 \equiv 35 \equiv 8 \pmod 9$

$4 \cdot 8 = 32 \equiv 5 \pmod 9$ ✓

11

a) $x \equiv 52 \cdot 4 \equiv 67 \pmod{141}$
$19 \cdot 67 = 1273 \equiv 4 \pmod{141}$ ✓

b) $x \equiv 34 \cdot 34 \equiv 1156 \equiv 88 \pmod{89}$
$88 \cdot 55 \equiv 4840 \equiv 34 \pmod{89}$ ✓

c) $x \equiv 73 \cdot 2 \equiv 146 \pmod{232}$
$146 \cdot 89 \equiv 12994 \equiv 2 \pmod{232}$ ✓

24

Solve Ex 21 using back substitution

21

$x \equiv 1 \pmod 2$
$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 4 \pmod{11}$

$x = a_1 M_1 y_1 + \dots + a_n M_n y_n$

$M = 2 \cdot 3 \cdot 5 \cdot 11 = 330$

$M_1 = \frac{330}{2} = 165$ $M_1 \equiv 165 \equiv 1 \pmod 2$ $y_1 = 1$

$M_2 = \frac{330}{3} = 110$ $M_2 \equiv 110 \equiv 2 \pmod 3$ $y_2 = 2$

$M_3 = \frac{330}{5} = 66$ $M_3 \equiv 66 \equiv 1 \pmod 5$ $y_3 = 1$

$M_4 = \frac{330}{11} = 30$ $M_4 \equiv 30 \equiv 8 \pmod{11}$ $y_4 = 7$

$x = 1 \cdot 165 \cdot 1 + 2 \cdot 110 \cdot 2 + 3 \cdot 66 \cdot 1 + 4 \cdot 30 \cdot 7$
$= 1643 \equiv 323 \pmod{330}$

31

a) use Fermat's little theorem to compute $5^{2003} \bmod 7$, $5^{2003} \bmod 11$, $5^{2003} \bmod 13$

b) use your results from part a and the Chinese remainder theorem to find $5^{2003} \bmod 1001$. (note: $1001 = 7 \cdot 11 \cdot 13$)

47

Show that 2821 is a Carmichael number

12
24
36
48
60
72
84
96