Number Theory

The Division "Algorithm"

- It's really just a *theorem*, not an algorithm…
  - Only called an "algorithm" for historical reasons.
- **Theorem:** For any integer *dividend* a and *divisor* $d \neq 0$, there is a unique integer *quotient* q and *remainder* $r \in \mathbf{N}$ such that $a = dq + r$ and $0 \leq r < |d|$. Formally, the theorem is: $\forall a,d \in \mathbf{Z}, d \neq 0: \exists! q,r \in \mathbf{Z}: 0 \leq r < |d|, a = dq + r$.
- We can find q and r by: $q = \lfloor a/d \rfloor$, $r = a - qd$.
  $q = a$ *div* d, $r = a$ *mod* d

The **mod** Operator

- An integer "division remainder" operator.
- Let $a,d\in\mathbf{Z}$ with $d\geq 1$. Then a **mod** d denotes the remainder r from the division "algorithm" with dividend a and divisor d; *i.e.* the remainder when a is divided by d.
- We can compute (a **mod** d) by: $a - d\cdot\lfloor a/d\rfloor$.

$$\boxed{\begin{array}{l} \mathbf{d\geq 1} \\ \mathbf{0 \leq (a \bmod d) < d} \end{array}}$$

$\in\mathbf{Z}$

Modular Congruence

- Let $a,b \in \mathbf{Z}$, $m \in \mathbf{Z}^+$.

  Where $\mathbf{Z}^+ = \{n \in \mathbf{Z} \mid n > 0\} = \mathbf{N} - \{0\}$ (the + integers).
- Then *a is congruent to b modulo m*, written "$a \equiv b \pmod{m}$", iff $m \mid a-b$.
  - Note: this is a different use of "≡" than the meaning "is defined as" I've used before.
- It's also equivalent to: $(a-b) \bmod m = 0$.

Useful Congruence Theorems

- **Theorem 3:** Let $a,b\in\mathbf{Z}$, $m\in\mathbf{Z}^+$. Then:
  $\boldsymbol{a\equiv b \pmod{m} \Leftrightarrow a \bmod m = b \bmod m}$.
- **Theorem 4:** Let $a,b\in\mathbf{Z}$, $m\in\mathbf{Z}^+$. Then:
  $a\equiv b \pmod{m} \Leftrightarrow \exists k\in\mathbf{Z}\ a=b+km$.
- **Theorem 5:** Let $a,b,c,d\in\mathbf{Z}$, $m\in\mathbf{Z}^+$. Then if $a\equiv b \pmod{m}$ and $c\equiv d \pmod{m}$, then:
  - $a+c \equiv b+d \pmod{m}$, and
  - $ac \equiv bd \pmod{m}$

Corollary 2

- Let m be a positive integer and a and b be integers. Then

$$(a+b) \bmod m = ((a \bmod m)+(b \bmod m)) \bmod m$$

and

$$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$$

Modular Exponentiation Problem

- **Problem:** Given large integers b (base), n (exponent), and m (modulus), efficiently compute $b^n \bmod m$.

Modular Exponentiation

- Note that:

$$b^n = b^{\overbrace{n_{k-1}\cdot 2^{k-1} + n_{k-2}\cdot 2^{k-2} + \ldots + n_0 \cdot 2^0}^{\text{The binary expansion of } n}}$$

$$= b^1 = b$$

$$= (b^{2^{k-1}})^{n_{k-1}} \times (b^{2^{k-2}})^{n_{k-2}} \times \ldots \times (b^{2^0})^{n_0}$$

- We can compute *b* to various powers of 2 by repeated squaring.
  - Then multiply them into the partial product, or not, depending on whether the corresponding n_i bit is 1.
- Crucially, we can do the **mod** *m* operations as we go along, because of the various identity laws of modular arithmetic. – All the numbers stay small.

Modular Exponentiation

$$b^n = (b^{2^{k-1}})^{n_{k-1}} \times (b^{2^{k-2}})^{n_{k-2}} \times \cdots \times (b^{2^0})^{n_0}$$

$x = 1$

$b_0 = b \; mod \; m$

$if \;\; n_0 = 1:$

$\quad x = (x * b_0) \; mod \; m$

$\forall (1 \le i \le k-1):$

$\quad b_i = (b_{i-1} \cdot b_{i-1}) \; mod \; m$

$\quad if \; n_i = 1:$

$\quad\quad x = (x * b_i) \; mod \; m$

Modular Exponentiation

procedure *modularExponentiation*(b: integer,
$n = (n_{k-1}\ldots n_0)_2$, m: positive integers)
$x := 1$ {result will be accumulated here}
$b^{2^i} := b$ **mod** m { b^{2^i} **mod** m; i=0 initially}
for $i := 0$ to $k-1$ {go thru all k bits of n}
 if $n_i = 1$ **then** $x := (x \cdot b^{2^i})$ **mod** m
 $b^{2^i} := (b^{2^i} \cdot b^{2^i})$ **mod** m
return x

$$\boxed{b^{2^{i+1}} = b^{2 \cdot 2^i} = \left(b^{2^i}\right) \cdot \left(b^{2^i}\right)}$$

Example 12

- Use Algorithm 5 to find 3^{644} mod 645.
  - $644=(1010000100)_2$

$i = 0$: Because $a_0 = 0$, we have $x = 1$ and $power = 3^2 \bmod 645 = 9 \bmod 645 = 9$;

$i = 1$: Because $a_1 = 0$, we have $x = 1$ and $power = 9^2 \bmod 645 = 81 \bmod 645 = 81$;

$i = 2$: Because $a_2 = 1$, we have $x = 1 \cdot 81 \bmod 645 = 81$ and $power = 81^2 \bmod 645 = 6561 \bmod 645 = 111$;

$i = 3$: Because $a_3 = 0$, we have $x = 81$ and $power = 111^2 \bmod 645 = 12{,}321 \bmod 645 = 66$;

$i = 4$: Because $a_4 = 0$, we have $x = 81$ and $power = 66^2 \bmod 645 = 4356 \bmod 645 = 486$;

$i = 5$: Because $a_5 = 0$, we have $x = 81$ and $power = 486^2 \bmod 645 = 236{,}196 \bmod 645 = 126$;

$i = 6$: Because $a_6 = 0$, we have $x = 81$ and $power = 126^2 \bmod 645 = 15{,}876 \bmod 645 = 396$;

$i = 7$: Because $a_7 = 1$, we find that $x = (81 \cdot 396) \bmod 645 = 471$ and $power = 396^2 \bmod 645 = 156{,}816 \bmod 645 = 81$;

$i = 8$: Because $a_8 = 0$, we have $x = 471$ and $power = 81^2 \bmod 645 = 6561 \bmod 645 = 111$;

$i = 9$: Because $a_9 = 1$, we find that $x = (471 \cdot 111) \bmod 645 = 36$.

3^{644} mod 645 = 36

$$\boxed{power: b^{2^{i+1}}}$$

SECTION 4.2 Integer Representations and Algorithms

26. Use Algorithm 5 to find 11^{644} **mod** 645.

26. $11^{644} \bmod 645$

$644 = (1010000100)_2$

$i = 0, \quad x = 1, \quad power = 11^2 \bmod 645 = 121$

$i = 1, \quad x = 1, \quad power = 121^2 \bmod 645 = 451$

$i = 2, \quad x = 451, \quad power = 451^2 \bmod 645 = 226$

$i = 3, \quad x = 451, \quad power = 226^2 \bmod 645 = 121$

$i = 4, \quad x = 451, \quad power = 121^2 \bmod 645 = 451$

$i = 5, \quad x = 451, \quad power = 451^2 \bmod 645 = 226$

$i = 6, \quad x = 451, \quad power = 226^2 \bmod 645 = 121$

$i = 7, \quad x = (451 \cdot 121) \bmod 645 = 391, \quad power = 121^2 \bmod 645 = 451$

$i = 8, \quad x = 391, \quad power = 451^2 \bmod 645 = 226$

$i = 9, \quad x = (391 \cdot 226) \bmod 645 = 1$

$11^{644} \bmod 645 = 1$

SECTION 4.2 Integer Representations and Algorithms

26. Use Algorithm 5 to find 11^{644} **mod** 645.

26. $(644)_{10} = (1010000100)_2$.

$i=0$ $a_0=0$ $x=1$ $11^2 \bmod 645 = 121 \bmod 645 = 121$

$i=1$ $a_1=0$ $x=1$ $121^2 \bmod 645 = 451$

$i=2$ $a_2=1$ $x=451$ $451^2 \bmod 645 = 226$

$i=3$ $a_3=0$ $x=451$ $226^2 \bmod 645 = 121$

$i=4$ $a_4=0$ $x=451$ $121^2 \bmod 645 = 451$

$i=5$ $a_5=0$ $x=451$ $451^2 \bmod 645 = 226$

$i=6$ $a_6=0$ $x=451$ $226^2 \bmod 645 = 121$

$i=7$ $a_7=1$ $x=(451 \times 121) \bmod 645 = 391$ $121^2 \bmod 645 = 451$

$i=8$ $a_8=0$ $x=391$ $451^2 \bmod 645 = 226$

$i=9$ $a_9=1$ $x=(391 \times 226) \bmod 645 = 1$ 所以答案为1

$11^{644} \bmod 645$

$= 11^{(1010000100)_2} \bmod 645$

$= (11^{0\cdot 2^0}\cdot 11^{0\cdot 2^1}\cdot 11^{1\cdot 2^2}\cdot 11^{0\cdot 2^3}\cdot 11^{0\cdot 2^4}\cdot 11^{0\cdot 2^5}\cdot 11^{0\cdot 2^6}\cdot 11^{1\cdot 2^7}\cdot 11^{0\cdot 2^8}\cdot 11^{1\cdot 2^9}) \bmod 645$

$= (11^{2^2}\cdot 11^{2^7}\cdot 11^{2^9}) \bmod 645$

$= ((11^{2^2} \bmod 645)(11^{2^7} \bmod 645)(11^{2^9} \bmod 645)) \bmod 645$

$11^2 \bmod 645 = 121 \qquad 11^{2^2} \bmod 645 = (121 \bmod 645)(121 \bmod 645) \bmod 645 = 451$

$11^{2^2} \bmod 645 = 451 \qquad 11^{2^3} \bmod 645 = (451 \times 451) \bmod 645 = 226$

$11^{2^3} \bmod 645 = 226 \qquad 11^{2^4} \bmod 645 = 226^2 \bmod 645 = 121$

$11^{2^4} \bmod 645 = 121 \qquad 11^{2^5} \bmod 645 = 121^2 \bmod 645 = 451$

$\therefore\ 11^{2^6} \bmod 645 = 226$

$11^{2^7} \bmod 645 = 121$

$11^{2^8} \bmod 645 = 451$

$11^{2^9} \bmod 645 = 226$

$\therefore$ 原式 $= (451 \times 121 \times 226) \bmod 645$

$= 12333046 \bmod 645 = 12333046 - 645 \times 19121$

$= 1$

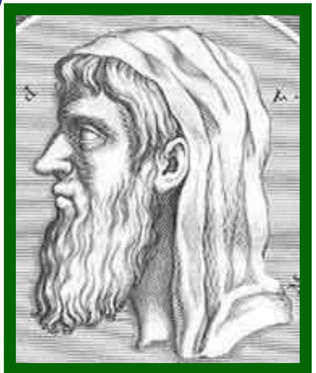
Greatest Common Divisor

- The *greatest common divisor* gcd(a,b) of integers a,b (not both 0) is the largest (most positive) integer d that is a divisor both of a and of b.

Relative Primality

- Integers a and b are called *relatively prime* or *coprime* iff their gcd = 1.
  - **Example:** Neither 21 nor 10 is prime, but they are *coprime*. 21=3·7 and 10=2·5, so they have no common factors > 1, so their gcd = 1.
- A *set* of integers $\{a_1, a_2, \ldots\}$ is *(pairwise) relatively prime* if all pairs (a_i, a_j), for $i \neq j$, are relatively prime.
  - Example: {10,17,21}

Euclid's Algorithm for GCD



Euclid of Alexandria 325-265 B.C.

- Finding GCDs by comparing prime factorizations can be difficult when the prime factors are not known!
- **Euclid discovered:** For all ints. a, b,

$$\gcd(a, b) = \gcd((a \bmod b), b).$$

- Sort a,b so that $a>b$, and then (given $b>1$) $(a \bmod b) < b$, so problem is simplified.

Euclidean Algorithm

- Suppose that a and b are positive integers with $a \geq b$.
  Let $r_0 = a$ and $r_1 = b$.
  Successive applications of the division algorithm yields:

$$
\begin{array}{ll}
r_0 = r_1 q_1 + r_2 & 0 \leq r_2 < r_1, \\
r_1 = r_2 q_2 + r_3 & 0 \leq r_3 < r_2, \\
\vdots & \\
r_{n-2} = r_{n-1} q_{n-1} + r_n & 0 \leq r_n < r_{n-1}, \\
r_{n-1} = r_n q_n. &
\end{array}
$$

- Eventually, a remainder of zero occurs in the sequence of terms: $a = r_0 > r_1 > r_2 > \cdots \geq 0$. The sequence can't contain more than a terms.
- By Lemma 1
  $\gcd(a,b) = \gcd(r_0,r_1) = \cdots = \gcd(r_{n-1},r_n) = \gcd(r_n, 0) = r_n$.
- Hence the greatest common divisor is the last nonzero remainder in the sequence of divisions.

GCDs as Linear Combinations

Bézout's Theorem: If a and b are positive integers, then there exist integers s and t such that $\gcd(a,b) = sa + tb$.

(*proof in exercises of Section* 5.2)

Definition: If a and b are positive integers, then integers s and t such that $\gcd(a,b) = sa + tb$ are called *Bézout coefficients* of a and b. The equation $\gcd(a,b) = sa + tb$ is called *Bézout's identity*.

- By Bézout's Theorem, the gcd of integers a and b can be expressed in the form $sa + tb$ where s and t are integers. This is a *linear combination* with integer coefficients of a and b.
  - $\gcd(6,14) = (-2)\cdot 6 + 1\cdot 14$

Finding GCDs as Linear Combinations

Example 17: Express gcd(252,198) = 18 as a linear combination of 252 and 198.

Solution: First use the Euclidean algorithm to show gcd(252,198) = 18

i. $252 = 1\cdot 198 + 54$
ii. $198 = 3\cdot 54 + 36$
iii. $54 = 1\cdot 36 + 18$
iv. $36 = 2\cdot 18$

- Now working backwards, from iii and ii above
  - $18 = 54 - 1\cdot 36$
  - $36 = 198 - 3\cdot 54$
- Substituting the 2nd equation into the 1st yields:
  - $18 = 54 - 1\cdot(198 - 3\cdot 54) = 4\cdot 54 - 1\cdot 198$
- Substituting $54 = 252 - 1\cdot 198$ (from i)) yields:
  - $18 = 4\cdot(252 - 1\cdot 198) - 1\cdot 198 = 4\cdot 252 - 5\cdot 198$

- This method illustrated above is a two pass method. It first uses the Euclidian algorithm to find the gcd and then works backwards to express the gcd as a linear combination of the original two integers.

Extended Euclidean Algorithm

It uses one pass through the steps of the Euclidean algorithm to find Bezout coefficients of a and b,

set $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, and $t_1 = 1$ and let

$$s_j = s_{j-2} - q_{j-1}s_{j-1} \text{ and } t_j = t_{j-2} - q_{j-1}t_{j-1}$$

for j = 2, 3, … , n, where the q_j are the quotients in the divisions used when the Euclidean algorithm finds gcd(a, b).

gcd(a,b) = sa + tb

$$\begin{array}{lll}
r_0 & = r_1q_1 + r_2 & 0 \le r_2 < r_1, \\
r_1 & = r_2q_2 + r_3 & 0 \le r_3 < r_2, \\
 & \vdots & \\
r_{n-2} & = r_{n-1}q_{n-1} + r_n & 0 \le r_n < r_{n-1}, \\
r_{n-1} & = r_nq_n. &
\end{array}$$

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}
0	252	198	1	54
1	198	54	3	36
2	54	36	1	18
3	36	18	2	0

EXAMPLE 18

- Express gcd(252, 198) = 18 as a linear combination of 252 and 198 using the extended Euclidean algorithm

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18	1	−1
3	36	18	2	0	−3	4
4					4	−5

$q_1 = 1$, $q_2 = 3$, $q_3 = 1$, and $q_4 = 2$

$s_0 = 1, s_1 = 0, t_0 = 0$, and $t_1 = 1$

$s_j = s_{j-2} - q_{j-1}s_{j-1}$ and $t_j = t_{j-2} - q_{j-1}t_{j-1}$

$$s_2 = s_0 - s_1q_1 = 1 - 0 \cdot 1 = 1,\ t_2 = t_0 - t_1q_1 = 0 - 1 \cdot 1 = -1,$$
$$s_3 = s_1 - s_2q_2 = 0 - 1 \cdot 3 = -3,\ t_3 = t_1 - t_2q_2 = 1 - (-1)3 = 4,$$
$$s_4 = s_2 - s_3q_3 = 1 - (-3) \cdot 1 = 4,\ t_4 = t_2 - t_3q_3 = -1 - 4 \cdot 1 = -5.$$

$$18 = 4 \cdot 252 - 5 \cdot 198$$

Solving Congruences

- A congruence of the form $ax \equiv b \pmod{m}$, where m is a positive integer, a and b are integers, and x is a variable, is called a linear congruence.
- One method uses an integer $\overline{a}$ such that $\bar{a}a \equiv 1 \bmod m$ if such an integer exists. Such an integer $\overline{a}$ is said to be an inverse （逆元） of a modulo m.

Inverse of *a* modulo *m*

- **Theorem 1**: If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists.

Proof: Since $\gcd(a,m) = 1$, there are integers s and t such that $sa + tm = 1$.

- Hence, $sa + tm \equiv 1 \pmod{m}$.
- Since $tm \equiv 0 \pmod{m}$, it follows that $sa \equiv 1 \pmod{m}$
- Consequently, s is an inverse of a modulo m.

Finding Inverses

Example: Find an inverse of 101 modulo 4620.

Solution: First use the Euclidian algorithm to show that gcd(101,4620) = 1.

Working Backwards:

$4620 = 45\cdot 101 + 75$
$101 = 1\cdot 75 + 26$
$75 = 2\cdot 26 + 23$
$26 = 1\cdot 23 + 3$
$23 = 7\cdot 3 + 2$
$3 = 1\cdot 2 + 1$
$2 = 2\cdot 1$

$1 = 3 - 1\cdot 2$
$1 = 3 - 1\cdot(23 - 7\cdot 3) = -1\cdot 23 + 8\cdot 3$
$1 = -1\cdot 23 + 8\cdot(26 - 1\cdot 23) = 8\cdot 26 - 9\cdot 23$
$1 = 8\cdot 26 - 9\cdot(75 - 2\cdot 26) = 26\cdot 26 - 9\cdot 75$
$1 = 26\cdot(101 - 1\cdot 75) - 9\cdot 75$
$= 26\cdot 101 - 35\cdot 75$
$1 = 26\cdot 101 - 35\cdot(4620 - 45\cdot 101)$
$= -35\cdot 4620 + 1601\cdot 101$

Since the last nonzero remainder is 1, gcd(101,4260) = 1

Bézout coefficients : − 35 and 1601

1601 is an inverse of 101 modulo 4620

Using Inverses to Solve Congruences

- **Example**: What are the solutions of the congruence $3x \equiv 4 (\bmod 7)$.
- **Solution**:

(1. Find an inverse of 3 modulo 7)

Because gcd(3,7) = 1, an inverse of 3 modulo 7 exists.

Using the Euclidean algorithm: $7 = 2 \cdot 3 + 1$.

From this equation, we get $-2 \cdot 3 + 1 \cdot 7 = 1$, and see that -2 and 1 are Bézout coefficients of 3 and 7.

Hence, -2 is an inverse of 3 modulo 7.

(Also every integer congruent to -2 modulo 7 is an inverse of 3 modulo 7, i.e., 5, -9, 12, etc.)

Using Inverses to Solve Congruences

- (2. Solve the congruence using the inverse)

Multiply both sides of the congruence by -2 giving

$$-2 \cdot 3x \equiv -2 \cdot 4 \pmod{7}.$$

Because $-6 \equiv 1 \pmod{7}$ and $-8 \equiv 6 \pmod{7}$, it follows that if x is a solution, then $x \equiv -8 \equiv 6 \pmod{7}$

- (3. Determine if every x with $x \equiv 6 \pmod{7}$ is a solution)

Assume that $x \equiv 6 \pmod{7}$. It follows that $3x \equiv 3 \cdot 6 = 18 \equiv 4 \pmod{7}$ which shows that all such x satisfy the congruence.

- (4. Conclusion)

The solutions are the integers x such that $x \equiv 6 \pmod{7}$.

6. Find an inverse of a modulo m for each of these pairs of relatively prime integers using the method followed in Example 2.

b) $a = 34, m = 89$

12. Solve each of these congruences using the modular inverses found in parts (b), (c), and (d) of Exercise 6.

a) $34x \equiv 77 \pmod{89}$

b) Euclidean Algorithm: $89 = 34 \cdot 2 + 21$ $\quad 34 = 21 \cdot 1 + 13$ $\quad 21 = 13 \cdot 1 + 8$ $\quad 13 = 8 \cdot 1 + 5$

$8 = 5 \cdot 1 + 3$ $\quad 5 = 3 \cdot 1 + 2$ $\quad 3 = 2 \cdot 1 + 1$ $\quad 2 = 1 \cdot 2$

Linear comb.: $1 = 3 - 2 = 3 - (5-3) = 3 \cdot 2 - 5 = (8-5) \cdot 2 - 5 = 8 \cdot 2 - 5 \cdot 3 = 8 \cdot 2 - (13-8) \cdot 3$

$= 8 \cdot 5 - 13 \cdot 3 = (21-13) \cdot 5 - 13 \cdot 3 = 21 \cdot 5 - 13 \cdot 8 = 21 \cdot 5 - (34-21) \cdot 8 = 21 \cdot 13 - 34 \cdot 8$

$= (89 - 34 \cdot 2) \cdot 13 - 34 \cdot 8 = 89 \cdot 13 - 34 \cdot 34$

So -34 is an inverse of 34 modulo 89

$-34 \cdot 34x \equiv -34 \cdot 77 \pmod{89}$

$x \equiv 52 \pmod{89}$

b) $89 = 2 \cdot 34 + 21$

$34 = 1 \cdot 21 + 13$

$21 = 1 \cdot 13 + 8$

$13 = 1 \cdot 8 + 5$

$8 = 1 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1$

$\therefore \gcd(34, 89) = 1$

$1 = 3 - 1 \cdot 2$

$= 3 - (5 - 1 \cdot 3) = -1 \cdot 5 + 2 \cdot 3$

$= -1 \cdot 5 + 2(8 - 1 \cdot 5) = 2 \cdot 8 - 3 \cdot 5$

$= 2 \cdot 8 - 3(13 - 1 \cdot 8) = -3 \cdot 13 + 5 \cdot 8$

$= -3 \cdot 13 + 5(21 - 1 \cdot 13) = 5 \cdot 21 - 8 \cdot 13$

$= 5 \cdot 21 - 8(34 - 1 \cdot 21) = -8 \cdot 34 + 13 \cdot 21$

$= -8 \cdot 34 + 13(89 - 2 \cdot 34)$

$= 13 \cdot 89 - 34 \cdot 34$

$s = -34$ and $t = 13$

$\therefore -34$ is an inverse of 34 modulo 89

-34 is an inverse of 34 modulo 89 (also 55)

$x \equiv 77 \cdot 55 = 4235 \equiv 52 \pmod{89}$

Check: $34 \cdot 52 = 1768 \equiv 77 \pmod{89}$