Integers and Algorithms

Find the GCD by prime factorization is time consuming.

The Euclidean Algorithm

Let $a = bq + r$,   all are integers, then:

$$GCD(a, b) = GCD(b, r)$$

If we apply this repeatedly then:

$$GCD(a, b) = ... = GCD(r_n, 0) = r_n$$

Details

Lemma: If a, b are integers not both zero then

$$GCD(a,b) = \begin{cases} GCD(b, a \text{ mod } b) & : \quad b \neq 0 \\ a & : \quad b = 0 \end{cases}$$

Proof. Let c be a common divisor of a and b. Since by Division algorithm $a = q \cdot b + a$ mod b then a mod $b = a - q \cdot b$ and thus $c|(a$ mod $b)$, so c is a common divisor of b and a mod b.

Euclidean Algorithm

Let $r_0 = a, r_1 = b$ and assume that $a \geq b$. By repeated application of the Division algorithm we get

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

Notation: GCD(a,b)=(a,b). Strictly decreasing sequence of nonnegative integers $a = r_0 \geq r_1 > r_2 \ldots, r_n \geq 0$(starting from r_1) terminates at 0 after at most a iterations. By the Lemma

$$(a, b) = (r_0, r_1)$$
$$= (r_1, r_2) = \ldots = (r_{n-1}, r_n) = (r_n, 0) = r_n.$$

Hence (a, b) is the last nonzero remainder.

Example: Find GCD(662,414)

$$662 = 414 \cdot 1 + 248$$
$$414 = 248 \cdot 1 + 166$$
$$248 = 166 \cdot 1 + 82$$
$$166 = 82 \cdot 2 + 2$$
$$82 = 2 \cdot 41 + 0$$

Therefore $GCD(662, 414) = 2$

Note: students should review the representations of integers using different bases.

Applications of Number Theory

Example: use the Fundamental Theorem of Arithmetic to show that $log_2 3$ is an irrational number.

Proof (by contradiction). Assume $log_2 3 = \frac{a}{b}$ therefore $3 = 2^{\frac{a}{b}}$ or $2^a = 3^b$ but this is impossible following the Fundamental Theorem of Arithmetic. Therefore $log_2 3$ cannot be written as $\frac{a}{b}$ or $log_2 3$ is irrational.

Theorem: a and b are integers then there exist integers s and t such that:

$$GCD(a, b) = sa + tb$$

(Bezout's identity).

Example: express $GCD(662, 414) = 2$ as a linear combination of 662 and 414.

To express $GCD(662, 414) = 2$ as a linear combination of 662 and 414 we backtrack the steps of the Euclidean algorithm.

$$2 = 166 - \underline{82} \cdot 2$$
$$\underline{82} = 248 - \underline{166} \cdot 1$$
$$\underline{166} = 414 - \underline{248} \cdot 1$$
$$\underline{248} = \underline{662} - \underline{414} \cdot 1$$

Backsubstitution gives:

$$
\begin{aligned}
GCD(662, 414) = 2 &= 166 - \underline{82} \cdot 2 \\
&= 166 - (248 - 166) \cdot 2 \\
&= \underline{166} \cdot 3 - 248 \cdot 2 \\
&= (\boxed{414} - 248) \cdot 3 - 248 \cdot 2 \\
&= \boxed{414} \cdot 3 - \underline{248} \cdot 5 \\
&= \boxed{414} \cdot 3 - (\boxed{662} - \boxed{414}) \cdot 5 \\
&= (\boxed{662})(-5) + (\boxed{414})(8)
\end{aligned}
$$

Therefore

$$GCD(662, 414) = (662)(-5) + (414)(8)$$

Lemma 1 (Euclid): If a, b, c are integers and $GCD(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Proof. We have by Bezout's identity

$$(a, b) = 1 = a \cdot s + b \cdot t.$$

Multiplying both sides by c we have

$$c = a(cs) + (bc)t.$$

Assumption $a|bc$ implies that a divides the RHS and thus it divides the LHS, i. e., $a \mid c$.

Lemma 2: (Generalization of Lemma 1) If p is prime and if $p \mid a_1 \cdot a_2 \cdots a_n$ where a_i are integers, then $p \mid a_i$ for some i.

Proof. To prove this Lemma use induction on n. The case $n = 1$ is trivial.

Assume that the result is true for n (induction hypothesis). Consider the product of $n+1$ integers $(a_1 \cdots a_n)a_{n+1} = ba_{n+1}$ that is divisible by p. By the Euclid's lemma $p|b$ or $p|a_{n+1}$. In the latter case we are done. In the former case by induction hypothesis $p|a_i$ for some $1 \leq i \leq n$.

Problem Prove that the decomposition of a composite into primes is unique. This is part of the Fundamental Theorem of Arithmetic.

Proof. We prove this by contradiction and Lemma 2. Assume that there are two different prime factorizations of n:

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$$

where $p_1 \leq \ldots \leq p_s$ and $q_1 \leq \ldots \leq q_t$ are all primes. Remove all common primes from the two factorizations to obtain

$$p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v}$$

where the primes on the LHS differ from the primes on the RHS, $u \geq 1$, $v \geq 1$ (because original factorizations were presumed to differ). However, by Lemma 2, $p_{i_1} | q_{j_k}$ for some k which is impossible, since q_{j_k} is prime that is different from p_{i_1}.

Theorem Let m be a positive integer, and a, b, c be integers. If $ac \equiv bc \pmod{m}$ and $GCD(c, m) = 1$ then $a \equiv b \pmod{m}$.

Proof.

$$ac \equiv bc \pmod{m} \iff$$
$$m|(ac - bc) \iff m|c(a - b)$$

Since $(c, m) = 1$ we have by Euclid's lemma

$$m|(a - b) \iff a \equiv b \pmod{m}.$$

Inverse of $a(\text{mod } m)$:
If $\bar{a}$ exists such that $\bar{a} \cdot a \equiv 1(\text{mod } m)$ we say $\bar{a}$ is an inverse of $a(\text{mod } m)$.

Linear Congruences

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

is called a linear congruence, m is a positive integer, a, b are integers, x is an integer variable.

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

Proof. Existence.

By Bezout's identity there exist integers s, t such that $GCD(a, m) = 1 = sa + tm$ thus $sa + tm \equiv 1 \pmod{m}$. Since $m|tm$ then $tm \equiv 0 \pmod{m}$ thus $sa \equiv 1 \pmod{m}$ or $s = \bar{a} \pmod{m}$.

Uniqueness.

Let $ba \equiv 1 \pmod m$. Since $\bar{a}a \equiv 1 \pmod m$ we have $ba - \bar{a}a = (b - \bar{a})a \equiv 0 \pmod m$. Since $(a, m) = 1$ Euclid's lemma implies $b - \bar{a} \equiv 0 \pmod m$ or $b \equiv \bar{a} \pmod m$.

<u>Example</u>: Find the inverse of 5 modulo 9.

$GCD(5, 9) = 1$ therefore inverse of
5 modulo 9 exists.
The Euclidean algorithm gives:

$$9 = 5 \cdot 1 + \underline{4}$$
$$5 = \underline{4} \cdot 1 + 1$$

Hence: $1 = 5 - \underline{4} = 5 - (9 - 5) = 2 \cdot 5 - 9$
Or: $1 \equiv 2 \cdot 5 \pmod 9$
Therefore 2 is the inverse of 5 modulo 9 .

Theorem: The solution to the linear congruence $ax \equiv b (\text{mod } m)$ exists if $GCD(a, m) = 1$.

If $GCD(a, m) = 1$ then $\bar{a}$ exists. Multiply both sides of the congruence by $\bar{a}$ to obtain

$$x \equiv \bar{a} \cdot b (\text{mod } m).$$

Problem: Solve the linear congruence $5x \equiv 3(\text{mod } 9)$.

Since 2 is an inverse of 5 modulo 9, multiply both sides of $5x \equiv 3(\text{mod } 9)$ by 2 we obtain:

$x \equiv 2 \cdot 3 = 6(\text{mod } 9)$

Chinese Remainder Theorem

Let $m_1, m_2, ..., m_n$ be pairwise relatively prime positive integers. The system:

$$x \equiv a_1 (\text{mod } m_1)$$
$$x \equiv a_2 (\text{mod } m_2)$$
$$.$$
$$.$$
$$.$$
$$x \equiv a_n (\text{mod } m_n)$$

has unique solution modulo $m = m_1 \cdot m_2 \cdots m_n$ (i. e., there is a solution x with $0 \leq x < m$ and all other solutions are congruent to $x \pmod{m}$.)

Proof. Existence.

Take $M_k = \frac{m}{m_k}, k = 1, \ldots, n$, so $M_k = \prod_{i=1, i \neq k}^{n} m_i$.
Since $(m_i, m_k) = 1$ for $i \neq k$ then $(m_k, M_k) = 1$ and

$$\exists y_k : y_k \equiv \overline{M}_k \pmod{m_k} \Longrightarrow M_k y_k \equiv 1 \pmod{m_k}.$$

We show that the solution is

$$x \equiv a_1 y_1 M_1 + \ldots + a_n y_n M_n \pmod{m}.$$

Since $M_j \equiv 0 \pmod{m_k}, j \neq k$
and $M_k y_k \equiv 1 \pmod{m_k}$ we have

$$x \equiv a_1 y_1 M_1 + \ldots + a_n y_n M_n$$
$$\equiv a_k M_k y_k \equiv a_k \pmod{m_k} \quad k = 1, \ldots, n.$$

Uniqueness.

Let $y = a_1 z_1 M_1 + \ldots + a_n z_n M_n$ be a solution to the system of congruences, where $z_k \equiv \overline{M}_k \pmod{m_k}$. Then

$$y \equiv a_k M_k z_k \equiv a_k \pmod{m_k}.$$

Hence

$$x - y \equiv 0 \pmod{m_k} \Longleftrightarrow x \equiv y \pmod{m}.$$

Example: solve the system of congruences

$$x \equiv 2 (\text{mod } 3)$$
$$x \equiv 3 (\text{mod } 5)$$
$$x \equiv 2 (\text{mod } 7)$$

$M_1 = 35, \quad M_2 = 21, \quad M_3 = 15$
$y_1 = 2, \quad y_2 = 1, \quad y_3 = 1$

$$x \equiv 2 \cdot 2 \cdot 35 + 3 \cdot 1 \cdot 21 + 2 \cdot 1 \cdot 15 (\text{mod } 105)$$

$$x \equiv 233 = 23 (\text{mod } 105)$$

Computing with Large Integers

Very large integers can be represented by a set of small integers. For example we can represent large integers by using moduli of $95, 97, 98, 99$. These numbers are pairwise relatively prime integers.

Example: 123684 can be represented by

$$123684 \bmod 99 = 33$$
$$123684 \bmod 98 = 8$$
$$123684 \bmod 97 = 9$$
$$123684 \bmod 95 = 89$$

Therefore 123684 is represented by $(33, 8, 9, 89)$.

Similarly
413456 is represented by $(32, 92, 42, 16)$.

Arithmetic on large integers can be done using these representations.

$123684 + 413456$ is equivalent to
$(33, 8, 9, 89) + (32, 92, 42, 16) =$
$(65 \bmod 99, 100 \bmod 98, 51 \bmod 97, 105 \bmod 95)$

$$= (65, 2, 51, 10)$$

To find the sum solve

$$x \equiv 65 (\text{mod } 99)$$
$$x \equiv 2 (\text{mod } 98)$$
$$x \equiv 51 (\text{mod } 97)$$
$$x \equiv 10 (\text{mod } 95)$$

Fermat Little Theorem

If p is a prime, a is an integer not divisible by p. Then

$$a^{p-1} \equiv 1 (\text{mod } p).$$

Furthermore for any $a \in Z$

$$a^p \equiv a (\text{mod } p).$$

There are integers which satisfy the FLT but are not prime. For example $341 = 11 \cdot 31$, but $2^{341-1} \equiv 1 \pmod{341}$.

Proof of Fermat Little Theorem

Define

$$\begin{aligned} R &= \{1, 2, \ldots, p-1\} \\ S &= \{ar \bmod p : r \in R\} \\ &= \{a \cdot 1 \bmod p, a \cdot 2 \bmod p, \ldots, a(p-1) \bmod p\}. \end{aligned}$$

If $r \in R$ and $ar \bmod p = 0$ then $r \bmod p = 0$, a contradiction. Therefore $0 \notin S$, and it follows that $S \subseteq R$. Let $r_1, r_2 \in R$. If $ar_1 \bmod p = ar_2 \bmod p$ then $ar_1 \equiv ar_2 \pmod p$ and so $r_1 \equiv r_2 \pmod p$. It follows that $r_1 = r_2$, since no two distinct members of R are congruent modulo p. Therefore $|S| = p - 1 = |R|$, and it follows that $S = R$. The product of the elements of R and the product of the elements of S must therefore be equal, so that

$$
\begin{aligned}
(p-1)! &= \prod_{r=1}^{p-1} (ar \bmod p) \\
&\equiv \prod_{r=1}^{p-1} ar \equiv a^{p-1}(p-1)! \pmod{p}.
\end{aligned}
$$

Because p is prime we have $p \not| (p-1)!$, hence $\gcd(p,(p-1)!) = 1$. Therefore

$$
\begin{aligned}
a^{p-1}(p-1)! &\equiv (p-1)! \pmod{p}, \\
a^{p-1} &\equiv 1 \pmod{p}.
\end{aligned}
$$

RSA Public Key Cryptosystem

(Rivest, Shamir, Adleman)

Step 1:
Translate text into large blocks of integers
Example: STOP $\rightarrow$ 1819 1415
each block is denoted by M.
Therefore a long text is translated into several blocks of integers denoted by $M's$.

Step 2: Encryption
Use two large primes p and q, $n = p \cdot q$, and an exponent e which is relatively prime to $(p-1)(q-1)$.
The encryption formula is:

$$C = M^e \bmod n$$

Each block of integers in Step 1 is encrypted by this formula.

Example: use $p = 43, q = 59$, $n = p \cdot q = 2537$
$e = 13$. Note that:
$GCD(e, (p-1)(q-1)) = GCD(13, 2436) = 1$
Therefore block 1 is encrypted as:
$C_1 \equiv 1819^{13} \bmod 2537 = 2081$
Block 2 is encrypted as:
$C_2 \equiv 1415^{13} \bmod 2537 = 2182$
The encrypted message is: 2081 2182

Step 3: Decryption

Knowing p, q, e we find d the inverse of e modulo $(p-1)(q-1)$
The decryption formula is:

$$P = C^d \bmod n.$$

Each encrypted block is decrypted by this formula.

Example: Continuing the example above we first calculate d using the table method.

n	q_n	r_n	s_n	t_n
0		2436	1	0
2	187	5	1	-187
3	2	3	-2	375
4	1	2	3	-562
5	1	1	-5	$\boxed{937}$
6	2	0	13	-2436

Thus we get $d = 937$, therefore the decrypted message for block 1 is:

$$P_1 = 2081^{937} \text{ mod } 2537 = 1819 \rightarrow ST$$

$$P_2 = 2182^{937} \text{ mod } 2537 = 1415 \rightarrow OP$$

Next we give the proof that RSA encryption method works.

Proof of RSA Scheme

Decryption key:

$$d \equiv \bar{e} \pmod{(p-1)(q-1)}$$

exists since $(e, (p-1)(q-1)) = 1$. Hence

$$de \equiv 1 \pmod{(p-1)(q-1)}$$

or

$$de = 1 + k(p-1)(q-1), \quad k \in Z.$$

Since $C = M^e$ mod n then $C \equiv M^e \pmod{n}$. Thus

$$C^d \equiv (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)}$$
$$= M \cdot M^{k(p-1)(q-1)}.$$

By Fermat's little theorem and assuming $(M, p) = (M, q) = 1$

$$M^{p-1} \equiv 1 \pmod{p}$$
$$M^{q-1} \equiv 1 \pmod{q}.$$

Hence

$$
\begin{aligned}
C^d &\equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1 \equiv M \pmod p \\
C^d &\equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \cdot 1 \equiv M \pmod q.
\end{aligned}
$$

Then since $(p, q) = 1$ it follows from CRT

$$M = C^d \mod pq.$$