Date: Monday, September 30, 2002
Prof.: Dr Jean-Yves Chouinard

Design of Secure Computer Systems CSI4138/CEG4394

Notes on the Modular Arithmetics and Galois Fields

1 Congruence and modular arithmetics

Let a, b, and n be non-negative integers, i.e. $n \in \mathcal{N}$ the set of natural numbers, and $n \neq 0$; then a is said to be congruent to b modulo n, that is

$$a \equiv_n b \qquad \text{if and only if,} \qquad a - b = kn$$

for some integer k. In other words, n divides the difference $(a - b)$. For instance,

$$17 \equiv_5 7 \qquad \text{since} \qquad 17 - 7 = 2 \times 5.$$

b is a residue of a modulo n and also a is a residue of b modulo n. For any modulus n, the set of integers $\{0, 1, \ldots, n-1\}$ forms a complete set of residues modulo n:

$$\{r_1, \ldots, r_n\} = \{0, 1, \ldots, n-1\}$$

The residue r of a modulo n is in the range $[0, n-1]$. Note that

$$a \bmod n = r \qquad \Rightarrow \qquad a \equiv_n r \qquad \text{but not the converse:}$$

$$a \equiv_n r \qquad \not\Rightarrow \qquad a \bmod n = r$$

meaning that $a \equiv_n r$ does not imply that $a \bmod n = r$; for instance,

$$17 \bmod 5 = 2 \qquad \Rightarrow \qquad 17 \equiv_5 2 \qquad \text{but}$$

$$17 \equiv_5 7 \qquad \not\Rightarrow \qquad 17 \bmod 5 = 7$$

1.1 Properties of modular arithmetics:

Let the symbol $(\odot)$ represent either an addition $(+)$ or a multiplication $(\times)$ operation.

1. Existence of identities:

$$\begin{aligned} a + 0 \bmod n &= 0 + a \bmod n = a \\ a \times 1 \bmod n &= 1 \times a \bmod n = a \end{aligned}$$

2. Existence of inverses:

$$\begin{aligned} a + (-a) \bmod n &= 0 \\ a \times (a^{-1}) \bmod n &= 1 \qquad \text{if } a \neq 0 \end{aligned}$$

3. Commutativity:

$$a \odot b \bmod n = b \odot a \bmod n$$

4. Associativity:

$$a \odot (b \odot c) \bmod n = (a \odot b) \odot c \bmod n$$

5. Distributivity:

$$a \times (b + c) \bmod n = [(a \times b) + (a \times c)] \bmod n$$

6. Reducibility:

$$\begin{aligned} (a \odot b) \bmod n &= [(a \bmod n) \odot (b \bmod n)] \bmod n \qquad \text{or equivalently:} \\ (a + b) \bmod n &= [(a \bmod n) + (b \bmod n)] \bmod n \\ (a \times b) \bmod n &= [(a \bmod n) \times (b \bmod n)] \bmod n \end{aligned}$$

- Ring: associativity and distributivity
- Commutative ring: associativity, distributivity, and commutativity
- Galois field: commutative ring where each element $\neq 0$ has a multiplicative inverse.

2 Principle of modular arithmetics (reducibility)

The reducibility property states that:

$$(a \odot b) \bmod n = [(a \bmod n) \odot (b \bmod n)] \bmod n$$

Proof:

Two integer numbers a_1 and a_2 can be written as: $a_1 = k_1 n + r_1$ and $a_2 = k_2 n + r_2$, where $r_1, r_2 \in [0, n-1]$, and both k_1 and k_2 are positive integers. The reducibility property can be proven for the addition operation $(\odot : +)$ as follow:

$$\begin{aligned} (a_1 + a_2) \bmod n &= [(k_1 n + r_1) + (k_2 n + r_2)] \bmod n \\ &= [(k_1 + k_2) n + r_1 + r_2)] \bmod n \\ &= (r_1 + r_2) \bmod n \\ (a_1 + a_2) \bmod n &= [(a_1 \bmod n) + (a_2 \bmod n)] \bmod n \end{aligned}$$

by definition of a residue. Similarly, for the multiplication operation, i.e. $(\odot : \times)$:

$$
\begin{aligned}
(a_1 \times a_2) \bmod n &= [(k_1 n + r_1) \times (k_2 n + r_2)] \bmod n \\
&= [(k_1 k_2 n^2) + (k_1 n r_2) + (k_2 n r_1) + (r_1 r_2)] \bmod n \\
&= [(k_1 k_2 n + k_1 r_2 + k_2 r_1) n + (r_1 r_2)] \bmod n \\
&= (r_1 \times r_2) \bmod n \\
(a_1 \times a_2) \bmod n &= [(a_1 \bmod n) \times (a_2 \bmod n)] \bmod n
\end{aligned}
$$

Principle of modular arithmetics

$$
\begin{array}{ccc}
a_1, a_2 & \longrightarrow \text{reduction modulo } n \longrightarrow & (a_1 \bmod n), (a_2 \bmod n) \\
\odot \downarrow & & \odot \downarrow \\
a_1 \odot a_2 & \longrightarrow \text{reduction modulo } n \longrightarrow & [(a_1 \bmod n) \odot (a_2 \bmod n)] \bmod n
\end{array}
$$

3 Modular exponentiation

Using the properties of modular arithmetics, modular exponentiation can be performed with the advantage of limiting the range of intermediate values:

$$
\begin{aligned}
e^t \bmod n &= [e \times e \times \ldots \times e] \bmod n \\
&= \{\underbrace{[e \bmod n]\ [e \bmod n]\ \ldots\ [e \bmod n]}_{t \text{ times}}\} \bmod n
\end{aligned}
$$

The intermediate values $[e \bmod n]$ being reduced within the range of the modulus, that is $[e \bmod n] \in [0, n-1]$.

$$
\boxed{e^t \bmod n = [\prod_{i=1}^{t} (e \bmod n)] \bmod n}
$$

Example*(modular exponentiation):*

Compute the following: $11^{207} \bmod 13$

$$
\begin{aligned}
11^{207} \bmod 13 &= \left[11^{128+64+8+4+2+1}\right] \bmod 13 \\
11^{207} \bmod 13 &= \left[11^{128} \times 11^{64} \times 11^{8} \times 11^{4} \times 11^{2} \times 11\right] \bmod 13 \\
11^{207} \bmod 13 &= \left\{\left[11^{128} \bmod 13\right] \left[11^{64} \bmod 13\right] \left[11^{8} \bmod 13\right] \left[11^{4} \bmod 13\right] \left[11^{2} \bmod 13\right] \times 11\right\} \bmod 13 \\
11^{207} \bmod 13 &= \left\{\left[11^{128} \bmod 13\right] \left[11^{64} \bmod 13\right] \left[11^{8} \bmod 13\right] \left[11^{4} \bmod 13\right] \times 4 \times 11\right\} \bmod 13 \\
11^{207} \bmod 13 &= \left\{\left[11^{128} \bmod 13\right] \left[11^{64} \bmod 13\right] \left[11^{8} \bmod 13\right] \times 3 \times 4 \times 11\right\} \bmod 13
\end{aligned}
$$

$$
\begin{aligned}
11^{207} \bmod 13 &= \left\{\left[11^{128} \bmod 13\right]\left[11^{64} \bmod 13\right] \times 9 \times 3 \times 4 \times 11\right\} \bmod 13 \\
11^{207} \bmod 13 &= \left\{\left[11^{128} \bmod 13\right] \times 3 \times 9 \times 3 \times 4 \times 11\right\} \bmod 13 \\
11^{207} \bmod 13 &= \{9 \times 3 \times 9 \times 3 \times 4 \times 11\} \bmod 13 \\
11^{207} \bmod 13 &= \{32076\} \bmod 13 \\
11^{207} \bmod 13 &= 5
\end{aligned}
$$

---

4 Multiplicative inverses

Let $a \in [0, n-1]$ and $x \in [0, n-1]$ be a multiplicative inverse of a such that:

$$\boxed{ax \bmod n = 1}$$

a has a unique multiplicative inverse modulo n when a and n are relatively prime or, in other words, if $\gcd(a, n) = 1$ ($\gcd(a, n)$: greatest common divisor of a and n).

Example*(multiplicative inverses):*

Let $a = 3$ and $n = 5$, then $\gcd(a, n) = 1$:

$$
\begin{aligned}
&a \times i \bmod 5 \\
3 \times 0 \bmod 5 &= 0 \\
3 \times 1 \bmod 5 &= 3 \\
3 \times 2 \bmod 5 &= 1 \\
3 \times 3 \bmod 5 &= 4 \\
3 \times 4 \bmod 5 &= 2
\end{aligned}
$$

There is a unique inverse for each value of a. The set of inverses $\{a_i^{-1}\}$ is in fact a permutation of the set of indices $\{i\}$. Now, changing n to $n = 6$:

$$
\begin{aligned}
&a \times i \bmod 6 \\
3 \times 0 \bmod 6 &= 0 \\
3 \times 1 \bmod 6 &= 3 \\
3 \times 2 \bmod 6 &= 0 \\
3 \times 3 \bmod 6 &= 3 \\
3 \times 4 \bmod 6 &= 0 \\
3 \times 5 \bmod 6 &= 3
\end{aligned}
$$

Since $\gcd(a,n) \neq 1$, the inverses of a are not unique.

If $\gcd(a,n) = 1$, then there exists an integer x, $0 < x < n$, such that:

$$\boxed{ax \bmod n = 1}$$

where, as stated above, the set $\{a \times i \bmod n\}$ is a permutation of $\{i\}$. The Euclid's algorithm can be used to compute to compute the greatest common divisor of a and n.

5 Euclid's algorithm

The following algorithm determines the greatest common divisor of two numbers, e.g. a and b:

$$\begin{aligned}
a &= b\, q_1 + r_1, && \text{for } 0 < r_1 < b \\
b &= r_1\, q_2 + r_2, && \text{for } 0 < r_2 < r_1 \\
r_1 &= r_2\, q_3 + r_3, && \text{for } 0 < r_3 < r_2 \\
r_2 &= r_3\, q_4 + r_4, && \text{for } 0 < r_4 < r_3 \\
&\vdots \\
r_{k-2} &= r_{k-1}\, q_k + r_k, && \text{for } 0 < r_k < r_{k-1} \\
r_{k-1} &= r_k\, q_{k+1}
\end{aligned}$$

The last remainder, r_k, is the greatest common divisor of a and b, i.e. $\gcd(a,b) = r_k$.

Example *($\gcd(a,b)$ using the Euclid's algorithm):*

For $a = 360$ and $b = 273$, determine their greatest common divisor $\gcd(a,b)$ by employing the Euclid's algorithm.

$$\begin{aligned}
360 &= 273 \times 1 + 87 \\
273 &= 87 \times 3 + 12 \\
87 &= 12 \times 7 + 3 \\
12 &= 3 \times 4
\end{aligned}$$

Therefore, the greatest common divisor $\gcd(360, 273)$ is equal to the remainder $r_3 = 3$. In fact, a and b can be written as:

$$\begin{aligned}
360 &= 5 \times 3 \times 3 \times 2 \times 2 \times 2, && \text{and} \\
273 &= 13 \times 7 \times 3
\end{aligned}$$

---

6 Inverse computation

Consider the *complete set* $\{r_i\}$ of residues modulo n:

$$\{r_1, \ldots, r_i, \ldots, r_n\} = \{0, \ldots, n-1\}$$

where r_i is a residue, such that $a \equiv_n r_i$. The *reduced set* of residues modulo n is defined as the subset of $\{r_i\}_{i=1,\ldots,n}$, such that r_i is relatively prime to n (excluding 0):

$$\{r_i\}_{i=1,\ldots,\phi(n)}$$

where $\phi(n)$ (called Euler totient function of n) represents the number of elements in this reduced set of residues. If

$$\gcd(a, n) = 1 \qquad \text{then} \qquad \gcd(ar_i, n) = 1$$

for the reduced set of residues $\{r_1, \ldots, r_{\phi(n)}\}$, then since (ar_i) is relatively prime with n:

$$(ar_i) \bmod n = r_j$$

In other words, the set $\{r_j\}$ is a permutation of the set $\{r_i\}$:

$$\{r_j\} = \{(ar_i) \bmod n\}_{i=1,\ldots,\phi(n)} = P \circ \{r_i\}_{i=1,\ldots,\phi(n)}$$

The following examples give the Euler totient function $\phi(n)$ for different values of n. For instance, if n is prime then, by definition: $\phi(n) = n - 1$. For $n = pq$ where p and q are primes:

$$\begin{aligned} \phi(n) &= \phi(pq) \\ \phi(n) &= (p-1)\ (q-1) \end{aligned}$$

Examples *(Euler totient function $\phi(n)$):*

For the following examples, let p, q and p_i be prime numbers while e and e_i are positive integers.

1. If $n = p$, then the reduced set of residues is:

$$\{r_i\} = \{1, 2, \ldots, p-1\}$$

whereas the Euler function is equal to:

$$\phi(n) = \phi(p) = p - 1$$

2. If $n = p^2$, the reduced set of residues is:

$$\{r_i\} = \{1, 2, \ldots, p-1, p+1, \ldots, 2p-1, 2p+1, \ldots, p^2-1\}$$

and,

$$\phi(n) = \phi(p^2) = p(p-1)$$

3. If $n = pq$, the reduced set of residues is:

$$\{r_i\} = \{1, 2, \ldots, pq-1\} - \{p, 2p, \ldots, (q-1)p\} - \{q, 2q, \ldots, (p-1)q\}$$

$$\phi(n) = \phi(pq) = (pq-1) - (q-1) - (p-1) = (p-1)(q-1)$$

4. If $n = p^e$, the reduced set of residues is:

$$\{r_i\} = \{1, 2, \ldots, p^e - 1\} - \{p, 2p, \ldots, (p^{e-1}-1)p\}$$

$$\phi(n) = \phi(p^e) = (p^e - 1) - (p^{e-1} - 1) = (p^{e-1})(p-1)$$

5. If $n = \prod_{i=1}^{t} p_i^{e_i}$, the Euler function is:

$$\phi(n) = \phi\left[\prod_{i=1}^{t} p_i^{e_i}\right] = \prod_{i=1}^{t} p_i^{(e_i-1)}\ (p_i - 1)$$

An integer n can always be expressed as a product of primes numbers:

$$\begin{aligned} n &= p_1^{e_1} \times p_2^{e_2} \times \ldots \times p_t^{e_t} \\ n &= \prod_{i=1}^{t} p_i^{e_i} \end{aligned}$$

where the p_i's are t distinct prime numbers and their exponents e_i are positive integers. As indicated above, the number of elements in the reduced set is given by:

$$\boxed{\phi(n) = \prod_{i=1}^{t} p_i^{(e_i-1)}\ (p_i - 1)}$$

6.1 Euler's generalization theorem

Euler's generalization theorem states that, for a and n (with $a < n$) such that $\gcd(a, n) = 1$:

$$\boxed{a^{\phi(n)} \bmod n = 1}$$

To show that $a^{\phi(n)} \bmod n = 1$, consider the reduced set of residues $\{r_i\}_{i=1,\ldots,\phi(n)}$ and the (permuted) set of residues $\{r_j\}$:

$$\begin{aligned} \{r_j\} &= \{a r_i \bmod n\}_{i=1,\ldots,\phi(n)} \\ \{r_j\} &= P \circ \{r_i\}_{i=1,\ldots,\phi(n)} \end{aligned}$$

Then the product of *all the elements* from the two reduced sets of residues, namely $\{r_i\}$ and $\{r_j\}$, must be equal:

$$\prod_{i=1}^{\phi(n)} r_i = \prod_{j=1}^{\phi(n)} r_j$$

Since the right-hand and left-hand sides of the equation are equal they should also be congruent modulo n:

$$\begin{aligned}
\prod_{j=1}^{\phi(n)} r_j &\equiv \prod_{i=1}^{\phi(n)} r_i \pmod n \\
\prod_{i=1}^{\phi(n)} (ar_i \bmod n) &\equiv \prod_{i=1}^{\phi(n)} r_i \pmod n \\
\prod_{i=1}^{\phi(n)} ar_i &\equiv \prod_{i=1}^{\phi(n)} r_i \pmod n \\
a^{\phi(n)} \prod_{i=1}^{\phi(n)} r_i &\equiv \prod_{i=1}^{\phi(n)} r_i \pmod n
\end{aligned}$$

because of the reducibility property. Dividing both sides by the factor $\prod_{i=1}^{\phi(n)} r_i$ leads to:

$$a^{\phi(n)} \equiv 1 \pmod n$$

and since $1 \in \{0, \ldots, n-1\}$ then:

$$a^{\phi(n)} \bmod n = 1$$

6.2 Fermat's little theorem

Fermat's little theorem states that if n is a prime number, with $a < n$, then:

$$\boxed{a^{n-1} \bmod n = 1}$$

by property of the Euler function of a prime number, i.e. $\phi(n) = n - 1$.

6.3 Multiplicative inverses

Consider the expression

$$ax \bmod n = 1$$

What is the multiplicative inverse x of a modulo n (assuming that $\gcd(a, n) = 1$)? By Euler's generalization theorem:

$$ax \bmod n = a^{\phi(n)} \bmod n = 1$$

which implies that:

$$\boxed{x = a^{\phi(n)-1} \bmod n}$$

Hence to compute an inverse a modular exponentiation program with the arguments $(a, [\phi(n) - 1], n)$ can be used. If n is a prime number, then $\phi(n) = n - 1$ (Fermat's theorem) and:

$$\boxed{x = a^{(n-1)-1} \bmod n = a^{n-2} \bmod n}$$

7 Galois Fields of Order p

Definition *(Galois Field of Order p):*
Let p be a prime number and $\mathbf{Z}_p = \{0, 1, \ldots, p-1\}$ be the set of residues modulo p. The finite (Galois) field $GF(p)$ is defined as the set $\mathbf{Z}_p$ with the arithmetics modulo p.

Example*(Galois Field modulo $p = 5$):*
Consider the Galois Field of order $p = 5$, i.e. $GF(5)$. Since $p = 5$ is a prime, the Galois field $GF(5)$ consists of $\mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$. The addition and multiplication operations in $GF(5)$ are given in Table 1 as well as the additive and multiplicative inverses, $-w$ and w^{-1}.

Table 1: Addition and multiplication operations in $GF(5)$.

Addition

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplication

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Inverses

w	$-w$	w^{-1}
0	0	
1	4	1
2	3	3
3	2	2
4	1	4
