Class Notes

for EE 7715

Part II

Instructor: Alex Skavantzos

E.E 7715

Basics of Number Theory

- Let a, b be two integers with b being a positive integer. The division of a by b is defined as $a = bq + r$; $0 \leq r < b$; where q is the quotient and r is the remainder or residue. If $r = 0$ (in which case $a = bq$), then b and q are factors or divisors of a. In this case we say that b divides a a fact that is denoted as $b \mid a$. If $r \neq 0$ then we say that b does not divide a and this is denoted as $b \nmid a$.

- If a number "a" has no other divisors (factors) except 1 and a, then "a" is called prime

- If a number is not prime, it is then a composite number

- Any composite number "a" can be factorized as

$a = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdots p_L^{e_L}$ where p_i's are prime numbers and $e_1, e_2, \ldots, e_L$ are integers. The fundamental theorem of arithmetic states that the above factorization is unique.

- The largest positive integer d which divides two integers a and b is called their greatest common divisor (G.C.D. or gcd) and is denoted as $d = (a, b)$.

If $d = (a, b) = 1$ (which means that a and b have no common factors (or divisors) other than 1), then a and b are called mutually prime or relatively prime or coprime.

- **Eucledian Algorithm for finding g.c.d**

Let a and b be integers. The Eucledian algorithm for finding (a, b) follows:

Divide a by b : $a = bq_1 + r_1$; If $r_1 = 0$ then $b = (a, b)$

Else divide b by r_1 : $b = r_1 q_2 + r_2$; if $r_2 = 0$ then $r_1 = (a, b)$

Else divide r_1 by r_2 : $r_1 = r_2 q_3 + r_3$

$$\vdots \qquad r_2 = r_3 q_4 + r_4$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$r_{k-2} = r_{k-1} \cdot q_k + r_k$$

$$r_{k-1} = r_k \cdot q_{k+1} + 0.$$

Then $r_k = (a, b) = g.c.d$ of a and b.

• **Lemma 1:** Let $d=(a,b)$ be the greatest common divisor of a and b. Then d is a linear combination of a and b or

$(a,b) = ma + nb$ where m, n are integers.

Proof: From the Eucledian algorithm used for finding the g.c.d we have

$$r_1 = a - bq_1 \quad (1)$$
$$r_2 = b - r_1 q_2 \quad (2)$$
$$r_3 = r_1 - r_2 q_3 \quad (3)$$
$$r_4 = r_2 - r_3 q_4 \quad (4)$$
$$\vdots$$
$$r_k = r_{k-2} - r_{k-1} q_k \quad (k)$$

Eq. (1) implies that r_1 is a linear combination of a and b. Equation (2) implies that r_2 is a linear combination of b and r_1 and thus r_2 is a linear combination of a and b. Similarly $r_3, r_4, \dots, r_k$ are linear combinations of a and b. Thus

$r_k = (a,b) = ma + nb$ where m, n integers

• Lemma 2: If $c|a$ and $c|b$ (ie; c is a common divisor of a and b), then $c|d$ where $d=(a,b)$.

Proof: Lemma 1 dictates that

$$d = ma + nb \quad (1)$$

$c|a$ implies $a = k\cdot c$ (2)

$c|b$ implies $b = \lambda\cdot c$ (3)

Eqs (1), (2), (3) yield

$$d = mkc + n\lambda c = (mk + n\lambda)c$$ which implies $c|d$.

• Lemma 3: If $c|a$ and $c|b$, then $c|ka \pm \lambda b$ or in other words c divides any linear combination of a and b.

Proof: $c|a$ implies $a = m\cdot c$ (1)

$c|b$ implies $b = n\cdot c$ (2)

Eqs. (1), (2) imply that $ka \pm \lambda b = k\cdot m\cdot c \pm \lambda\cdot n\cdot c = (km \pm \lambda n)c$. Thus $c|ka \pm \lambda b$.

- Rewriting the Eucledian algorithm for finding the g.c.d.

Let $\langle x \rangle_m$ denote the operation $x \bmod m$.

Let a and b be integers. The Euclidian algorithm for finding (a, b) follows

$$\langle a \rangle_b = r_1 \neq 0$$
$$\langle b \rangle_{r_1} = r_2 \neq 0$$
$$\langle r_1 \rangle_{r_2} = r_3 \neq 0$$
$$\langle r_2 \rangle_{r_3} = r_4 \neq 0$$
$$\vdots \quad \vdots$$
$$\langle r_{k-2} \rangle_{r_{k-1}} = r_k \neq 0$$
$$\langle r_{k-1} \rangle_{r_k} = 0.$$

Then the g.c.d of a and b is r_k or $r_k = (a, b)$.

Example 1: Using the Euclidean algorithm find (34, 21)

Solution: Here

$\langle 34 \rangle_{21} = 13 \neq 0$

$\langle 21 \rangle_{13} = 8 \neq 0$

$\langle 13 \rangle_{8} = 5 \neq 0$

$\langle 8 \rangle_{5} = 3 \neq 0$

$\langle 5 \rangle_{3} = 2 \neq 0$

$\langle 3 \rangle_{2} = 1 \neq 0$

$\langle 2 \rangle_{1} = 0$. Therefore $(34, 21) = 1$.

Example 2: Using the Euclidean algorithm find (75, 42)

Solution: Here

$\langle 75 \rangle_{42} = 33 \neq 0$; $\langle 42 \rangle_{33} = 9 \neq 0$;

$\langle 33 \rangle_{9} = 6 \neq 0$; $\langle 9 \rangle_{6} = 3 \neq 0$;

$\langle 6 \rangle_{3} = 0$. Therefore,

$(75, 42) = 3$.

(8) a

Problem 1: Prove that $(2^n - 1, 2^{n+1} - 1) = 1$; (n is integer).

Proof 1: Let d be a common divisor of $2^{n+1} - 1$ and $2^n - 1$. Then $d | 2^{n+1} - 1$ and $d | 2^n - 1$. According to Lemma 3, $d | (2^{n+1} - 1) - 2(2^n - 1)$ or $d | 2^{n+1} - 1 - 2^{n+1} + 2$ or $d | 1$. Thus d must be $d = 1$ and $(2^n - 1, 2^{n+1} - 1) = 1$.

Proof 2: We can also prove the above by using the Euclidean algorithm for finding the g.c.d. Just see that

$$\langle 2^{n+1} - 1 \rangle_{2^n - 1} = \langle 2 \times 2^n - 1 \rangle_{2^n - 1}$$

$$= \langle 2 \times \langle 2^n \rangle_{2^n - 1} - 1 \rangle_{2^n - 1} =$$

$$= \langle 2 \times 1 - 1 \rangle_{2^n - 1} = 1 \; ; \text{ and}$$

$\langle 2^n - 1 \rangle_1 = 0$. Thus $(2^n - 1, 2^{n+1} - 1) = 1$.

Problem 3: Prove that $(2^n-3, 2^n+1) = 1$.

Proof: Let d be a common divisor of 2^n-3 and 2^n+1. Then $d \mid 2^n-3$ and $d \mid 2^n+1$. According to Lemma 3

$$d \mid (2^n+1) - (2^n-3) \text{ or}$$

$d \mid 4$ or $d = 1, 2, 4$. But neither 2 nor 4 divide the odds 2^n-3 and 2^n+1. Thus the only common divisor of 2^n-3 and 2^n+1 is $d=1$ and therefore $(2^n-3, 2^n+1) = 1$.

• Summary of notations

- $a \mid b$ means a divides b
- $a \nmid b$ means a does not divide b
- (a, b) denotes the greatest common divisor of a and b
- $\langle x \rangle_m$ means $x \bmod m$

EE 7715 (1) b

Modular Arithmetic

Properties of the mod m operator

- $\langle x \pm y \rangle_m = \langle \langle x \rangle_m \pm \langle y \rangle_m \rangle_m$

Example: $\langle 17+19 \rangle_7 = \langle \langle 17 \rangle_7 + \langle 19 \rangle_7 \rangle_7$

$= \langle 3+5 \rangle_7 = \langle 8 \rangle_7 = 1.$

- $\langle xy \rangle_m = \langle \langle x \rangle_m \langle y \rangle_m \rangle_m$

- Additive Inverse mod m

$\langle -a \rangle_m = \langle m-a \rangle_m$

Obviously, $\langle -a \rangle_m$ is a number such that

$\langle -a + a \rangle_m = 0.$

Example: $\langle -3 \rangle_7 = \langle 7-3 \rangle_7 = \langle 4 \rangle_7 = 4.$

Also, $\langle -a \rangle_m = \langle -\langle a \rangle_m \rangle_m$.

Example: $\langle -40 \rangle_{13} = \langle -\langle 40 \rangle_{13} \rangle_{13}$

$= \langle -1 \rangle_{13} = \langle 13-1 \rangle_{13} = 12$

• Congruent numbers modulo m

The integer numbers a and b are called congruent modulo m if $\langle a \rangle_m = \langle b \rangle_m$. This can also be denoted by $\langle a = b \rangle_m$ or $a = b \bmod m$. In this case $m \mid a-b$.

Example: $a = 35$, $b = 15$, $m = 10$.

Here $\langle a \rangle_m = \langle 35 \rangle_{10} = 5$ and $\langle b \rangle_m = \langle 15 \rangle_{10} = 5$. Thus 35 and 15 are congruent mod 10 and 10 divides their difference or $10 \mid 35-15$.

• Multiplicative Inverse mod m

The multiplicative inverse of a mod m is denoted as $\langle a^{-1} \rangle_m$.

$\langle a^{-1} \rangle_m = b$, $b \in \{0, 1, 2, \cdots, m-1\}$ where

b is such that $\langle a\,b \rangle_m = 1$

- $\langle a^{-1} \rangle_m = \langle (\langle a \rangle_m)^{-1} \rangle_m$.

Example:

- $\langle 5^{-1} \rangle_{11} = 9$; (observe that $\langle 5 \times 9 \rangle_{11} = 1$).
- $\langle 3^{-1} \rangle_9$ does not exist

- $\langle 5^{-1} \rangle_{20}$ does not exist
- $\langle 17^{-1} \rangle_{11} = \langle (\langle 17 \rangle_{11})^{-1} \rangle_{11} = \langle 6^{-1} \rangle_{11} = 2$;

  (observe that $\langle 17 \times 2 \rangle_{11} = \langle 34 \rangle_{11} = 1$).
- $\langle 4^{-1} \rangle_{19} = 5$

Question: When does $\langle a^{-1} \rangle_m$ exist?

Answer: $\langle a^{-1} \rangle_m$ exists if and only if $(a, m) = 1$; (in other words $\langle a^{-1} \rangle_m$ exists if and only if a and m are relatively prime)

Question: Whenever $\langle a^{-1} \rangle_m$ exists, how do we find $\langle a^{-1} \rangle_m$? Is it by trial and error?

Answer: No. There is a closed formula that provides the multiplicative inverse. This formula relates to Euler's totient function (or phi-function)

Euler's totient function (phi-function)

Consider a positive integer m. Define $\phi(m)$ to be the number of positive integers that are smaller than m and also relatively prime to m; ($\phi(m)$ is called Euler's totient function or phi-function).

Then

- If p is positive prime then $\boxed{\phi(p) = p-1}$
- If $m = p^e$ where $m > 0$ and p = prime then $\boxed{\phi(p^e) = p^{e-1}(p-1)}$
- If $(a, b) = 1$ then $\boxed{\phi(ab) = \phi(a)\phi(b)}$
- If m = composite and $m = p_1^{e_1} \cdot p_2^{e_2} \cdots p_L^{e_L}$ where $p_1, p_2, \ldots, p_L$ are primes and $e_1, e_2, \ldots, e_L$ are integers, then

$$\phi(m) = \phi(p_1^{e_1} p_2^{e_2} \cdots p_L^{e_L}) = p_1^{e_1-1} \cdot (p_1-1) \cdot p_2^{e_2-1}(p_2-1) \cdots p_L^{e_L-1}(p_L-1)$$

• Euler's Theorem

If $(a, m) = 1$; (a and m are relatively prime), $m > 0$, then

$$\boxed{\langle a^{\phi(m)} \rangle_m = 1}$$

• Fermat's Theorem

This is a special case of Euler's theorem. It states:

If p = prime and $(a, p) = 1$, then

$$\boxed{\langle a^{p-1} \rangle_p = 1}$$

Usefulness of Euler's and Fermat's Theorems

Euler's and Fermat's theorems are useful since they provide closed formulas for computing the multiplicative inverse.

Recall that Euler's theorem says that if $(a, m) = 1$ then $\langle a^{\phi(m)} \rangle_m = 1 = \langle a^0 \rangle_m$

- Thus $\langle a^{-1} \rangle_m = \langle a^{\phi(m)-1} \rangle_m$

Fermat's theorem states that if p = prime and $(a, p) = 1$ then $\langle a^{p-1} \rangle_p = 1 = \langle a^0 \rangle_p$.

Thus $\langle a^{-1} \rangle_p = \langle a^{p-2} \rangle_p$ where p = prime, $(a, p) = 1$

Example 1: Find $\phi(p)$ where $p = 7$.

Answer: $p = 7$ is prime. Thus $\phi(7) = 7 - 1 = 6$. Indeed the six numbers $1, 2, \ldots, 6$ are smaller than 7 and relatively prime to 7

Example 2: Find $\phi(m)$ where $m = 36$.

Answer: $m = 2^2 \times 3^2$; (2 and 3 are primes). Then $\phi(m) = \phi(36) = \phi(2^2 \times 3^2) = \phi(2^2) \times \phi(3^2) = 2^{2-1} \times (2-1) \times 3^{2-1} \times (3-1)$ $= 2 \times 1 \times 3 \times 2 = 12$. Thus, there are twelve numbers smaller than 36 and relatively prime to 36. These #s are: $1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35$.

Example 3: Find $\langle 6^{-1} \rangle_{11}$.

Here $(6, 11) = 1$ and thus $\langle 6^{-1} \rangle_{11}$ exists. The number $p = 11$ is prime and therefore Fermat's theorem dictates

$$\langle 6^{-1}\rangle_{11} = \langle 6^{11-2}\rangle_{11} = \langle 6^9\rangle_{11}$$

$$= \langle (6^2)^4 \cdot 6\rangle_{11} = \langle (\langle 6^2\rangle_{11})^4 \cdot 6\rangle_{11} =$$

$$= \langle 3^4 \times 6\rangle_{11} = \langle 81 \times 6\rangle_{11} = \langle \langle 81\rangle_{11} \times 6\rangle_{11}$$

$$= \langle 4 \times 6\rangle_{11} = \langle 24\rangle_{11} = 2.$$ Thus

$\boxed{\langle 6^{-1}\rangle_{11} = 2}$. Double check to see that

$\langle 6 \times 2\rangle_{11} = \langle 12\rangle_{11} = 1$.

Example 4: Find $\langle 5^{-1}\rangle_{36}$.

Answer: Here $(5, 36) = 1$ and thus $\langle 5^{-1}\rangle_{36}$ exists. The number 36 is composite. Euler's theorem dictates that $\langle 5^{-1}\rangle_{36} = \langle 5^{\phi(36)-1}\rangle_{36}$. In example 2 we found that $\phi(36) = 12$. Therefore,

$$\langle 5^{-1}\rangle_{36} = \langle 5^{12-1}\rangle_{36} = \langle 5^{11}\rangle_{36}$$

$$= \langle (5^3)^3 \times 5^2\rangle_{36} = \langle 125^3 \times 5^2\rangle_{36} =$$

(10) b

$= \langle (\langle 125 \rangle_{36})^3 \times 5^2 \rangle_{36} = \langle 17^3 \times 5^2 \rangle_{36} =$

$= \langle 17^2 \times 17 \times 5^2 \rangle_{36} = \langle 289 \times 17 \times 5^2 \rangle_{36}$

$= \langle \langle 289 \rangle_{36} \times 17 \times 5^2 \rangle_{36} = \langle 1 \times 17 \times 5^2 \rangle_{36}$

$= \langle 17 \times 5 \times 5 \rangle_{36} = \langle 85 \times 5 \rangle_{36} = \langle \langle 85 \rangle_{36} \times 5 \rangle_{36}$

$= \langle 13 \times 5 \rangle_{36} = \langle 65 \rangle_{36} = 29.$

Thus $\langle 5^{-1} \rangle_{36} = 29$. Double check to see that $\langle 5 \times 29 \rangle_{36} = \langle 145 \rangle_{36} = 1$.

Note: On page 4 of this handout we stated the necessary and sufficient condition for the existence of $\langle a^{-1} \rangle_m$. Let's now prove half of this condition.

•• Prove that if $(a, m) = d \neq 1$ then $\langle a^{-1} \rangle_m$ does not exist.

Proof:

Assume that $\langle a^{-1} \rangle_m$ exists. Then

$\langle a^{-1} \times a \rangle_m = 1$ or $\boxed{a^{-1} \cdot a = q \cdot m + 1}$ (1)

Since $d = (a, m)$ then $d|a$ and $d|m$.

Therefore

$a = k_1 d$ (2)

$m = k_2 d$ (3) ; here k_1, k_2 are integers.

Then eqs. (1), (2), (3) imply

$\boxed{a^{-1} k_1 d = q k_2 d + 1}$ (4)

Taking both sides of eq. (4) modulo d and considering the fact that $d \neq 1$ yields

$\langle a^{-1} k_1 d \rangle_d = \langle q k_2 d + 1 \rangle_d$ or $\boxed{0 = 1}$ (5).

Eq. (5) is a contradiction which occured due to the wrong assumption that $\langle a^{-1} \rangle_m$ exists. Therefore $\langle a^{-1} \rangle_m$ does <u>not</u> exist.

EE 7715

Modular fields and rings

• Let p be a prime number. Then the set $Z_p = \{0, 1, 2, 3, \cdots, p-1\}$ equipped with the operations addition mod p, subtraction mod p, multiplication mod p forms the finite field of integers modulo p. We can denote this field by $\{Z_p ; \langle +/- \rangle_p ; \langle \times \rangle_p\}$.

•• Let c be a composite number. Then the set $Z_c = \{0, 1, 2, \cdots, c-1\}$ equipped with the operations addition mod c, subtraction mod c, multiplication mod c forms a finite ring which is the ring of integers modulo c. We can denote this ring by $\{Z_c ; \langle +/- \rangle_c ; \langle \times \rangle_c\}$.

Properties of modular fields and rings.

• Properties of modular fields:

Let p be a prime # and let $Z_p = \{0, 1, \cdots, p-1\}$ be the field of integers mod p. Then,

→ If $a \in Z_p$, $b \in Z_p$ then $\langle a \odot b \rangle_p \in Z_p$ where $\odot = +, -, \times$.

(2) c

→ For any element $a \in Z_p$, its additive inverse $\langle -a \rangle_p$ always exists and it is an element of Z_p (i.e; $\langle -a \rangle_p \in Z_p$).

→ For any <u>nonzero</u> element $a \in Z_p$ ($a \neq 0$), its multiplicative inverse $\langle a^{-1} \rangle_p$ exists and is an element of Z_p (i.e; $\langle a^{-1} \rangle_p \in Z_p$).

→ There exists <u>at least one</u> generator g for the modular field Z_p <u>which generates all its nonzero elements</u>. The generator $g \in Z_p$ and $\langle g^0 \rangle_p, \langle g^1 \rangle_p, \langle g^2 \rangle_p, \cdots, \langle g^{p-2} \rangle_p$ generate <u>all the non zero elements of Z_p.</u>

●● <u>Properties of modular rings:</u>

Let c be a composite # and let $Z_c = \{0, 1, \cdots, c-1\}$ be the ring of integers mod c. Then:

→ $a \in Z_c, b \in Z_c \Rightarrow \langle a \odot b \rangle_c \in Z_c$ where $\odot = +, -, \times$.

→ If $a \in Z_c$, then $\langle -a \rangle_c$ exists and $\langle -a \rangle_c \in Z_c$.

→ <u>Not</u> every nonzero element of Z_c has a multiplicative inverse in Z_c.

→ There <u>does not exist any generator</u> that can generate the <u>entire</u> modular ring Z_c.

EE 7715 (3) C

Generators of Modular fields

Let p be a prime number and let $Z_p = \{0, 1, \cdots, p-1\}$ be the field of integers modulo p.

There exists at least one generator g for the modular field Z_p which generates all its non zero elements. The generator g belongs to Z_p ($g \in Z_p$) and $\langle g^0 \rangle_p$, $\langle g^1 \rangle_p$, $\langle g^2 \rangle_p$, $\cdots$, $\langle g^{p-2} \rangle_p$ are all the non zero elements of Z_p. The following hold true:

- $\langle g^i \rangle_p \neq 1$ for $0 < i < p-1$.
- $\langle g^{\frac{p-1}{2}} \rangle_p = \langle -1 \rangle_p$.
- If g is a generator of Z_p and $\frac{p-1}{2}$ is even then $\langle -g \rangle_p$ is also a generator of Z_p.
- If g is a generator of Z_p then $\langle g^{-1} \rangle_p$ is also a generator of Z_p.

Example: Find the generators of Z_{17}.

$Z_{17} = \{0, 1, 2, \cdots, 16\}$

Obviously 0 is not a generator.

1 is not a generator since $\langle 1^i \rangle_p = 1$

$\langle -1 \rangle_{17} = 16$ is not a generator since the numbers generated are $1, \langle -1 \rangle_{17}, 1, \langle -1 \rangle_{17} \cdots$

Let's now try 2. $\langle 2^0 \rangle_{17} = 1$, $\langle 2^1 \rangle_{17} = 2$, $\langle 2^2 \rangle_{17} = 4$, $\langle 2^3 \rangle_{17} = 8$, $\langle 2^4 \rangle_{17} = 16 = \langle -1 \rangle_{17}$.

Thus $\langle 2^8 \rangle_{17} = 1$ and 2 is not generator.

The number 4 is also not a generator since $\langle 4^4 \rangle_{17} = \langle 2^8 \rangle_{17} = 1$

Also, $\langle -4 \rangle_{17} = 13$ can not be a generator since $\langle (-4)^4 \rangle_{17} = \langle 4^4 \rangle_{17} = 1$

Next we can try 3

↳ go to next page

(5) c

$\langle 3^0 \rangle_{17} = 1$ $\quad$ $\langle 3^8 \rangle_{17} = \langle 33 \rangle_{17} = \langle -1 \rangle_{17} = 16$

$\langle 3^1 \rangle_{17} = 3$ $\quad$ $\langle 3^9 \rangle_{17} = \langle -3 \rangle_{17} = 14$

$\langle 3^2 \rangle_{17} = 9$ $\quad$ $\langle 3^{10} \rangle_{17} = \langle -9 \rangle_{17} = 8$

$\langle 3^3 \rangle_{17} = 10$ $\quad$ $\langle 3^{11} \rangle_{17} = \langle -10 \rangle_{17} = 7$

$\langle 3^4 \rangle_{17} = 13$ $\quad$ $\langle 3^{12} \rangle_{17} = \langle -13 \rangle_{17} = 4$

$\langle 3^5 \rangle_{17} = 5$ $\quad$ $\langle 3^{13} \rangle_{17} = \langle -5 \rangle_{17} = 12$

$\langle 3^6 \rangle_{17} = 15$ $\quad$ $\langle 3^{14} \rangle_{17} = \langle -15 \rangle_{17} = 2$

$\langle 3^7 \rangle_{17} = 11$ $\quad$ $\langle 3^{15} \rangle_{17} = \langle -11 \rangle_{17} = 6$

Thus 3 is a generator of Z_{17}.

Since $\frac{p-1}{2} = \frac{17-1}{2} = 8 =$ even, then $\langle -3 \rangle_{17} = 14$ is also a generator.

$\langle 3^{-1} \rangle_{17} = 6$ is also a generator.

Also $\langle -6 \rangle_{17} = 11$ is generator.

The number 9 can not be a generator since $\langle 9^8 \rangle_{17} = \langle (3^2)^8 \rangle_{17} = \langle 3^{16} \rangle_{17} = 1$.

6 c

Also, $\langle -9 \rangle_{17} = 8$ is not a generator since $\langle (-9)^8 \rangle_{17} = \langle 9^8 \rangle_{17} = 1$.

Trying number 5 one can easily see that 5 is a generator ($\langle 5^0 \rangle_{17}, \langle 5^1 \rangle_{17}, \cdots, \langle 5^{15} \rangle_{17}$ are all the non zero elements of Z_{17}).

Thus $\langle -5 \rangle_{17} = 12$ is also a generator (since $\frac{p-1}{2} = \frac{17-1}{2} = 8 = \text{even}$)

$\langle 5^{-1} \rangle_{17} = 7$ is another generator.

Also, $\langle -7 \rangle_{17} = 10$ is generator.

The eight generators of Z_{17} are:

3, 5, 6, 7, 10, 11, 12, 14.

Usefulness of generators

Using generators, the multiplication mod p (p = prime) can be translated into addition. This technique is called index calculus technique

Consider the field Z_p (p = prime). Let $a, b \in Z_p$ and let g be one generator of Z_p.

Then $a = \langle g^i \rangle_p$; $b = \langle g^j \rangle_p$

Thus $$\langle a \times b \rangle_p = \langle g^{\langle i+j \rangle_{p-1}} \rangle_p .$$

Example: Consider Z_{17}. One generator of Z_{17} is $g = 3$. Let $a = 4$, $b = 12$. Then,

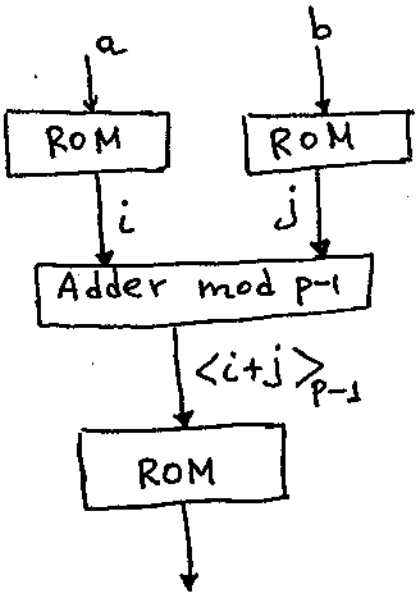
$a = 4 = \langle 3^{12} \rangle_{17}$ and $b = 12 = \langle 3^{13} \rangle_{17}$.

Thus $\langle a \times b \rangle_{17} = \langle 3^{\langle 12+13 \rangle_{16}} \rangle_{17} =$

$= \langle 3^{\langle 25 \rangle_{16}} \rangle_{17} = \langle 3^9 \rangle_{17} = 14.$

Implementation of the index calculus technique

A possible implementation of the index calculus technique which relies on ROM tables is shown below:



$$\left\langle g^{\langle i+j \rangle_{p-1}} \right\rangle_p = \langle a \times b \rangle_p$$

* p = prime

$a, b \in Z_p$

$a = \langle g^i \rangle_p \; j$

$b = \langle g^j \rangle_p$

EE 7715

Introduction to the Residue Number System (RNS)

A Residue Number System (RNS) is defined by a set $S = \{m_1, m_2, m_3, \cdots, m_L\}$ which is called the set of moduli. The moduli $m_1, m_2, \cdots, m_L$ are positive integers such that $(m_i, m_j) = 1$ for $i \neq j$ (ie; the moduli are pairwise relatively prime or relatively prime in pairs).

Let M be $M = \prod_{i=1}^{L} m_i = m_1 \cdot m_2 \cdots m_L$

Then any integer $X \in Z_M$ ($Z_M = \{0, 1, \cdots, M-1\}$ is the ring of integers modulo M) has a unique RNS representation

$$X \xrightarrow{RNS} (X_1, X_2, X_3, \cdots, X_L)$$

where

$$X_i = \langle X \rangle_{m_i} \quad \text{if } X > 0$$

$$X_i = \langle M - |X| \rangle_{m_i} \quad \text{if } X < 0 .$$

The above dictates the weighted-to-RNS conversion.

- Processing in the RNS domain

$X, Y \in Z_M$; $Z_M = \{0, 1, 2, \cdots, M-1\}$ = ring of integers mod M ; $M = \prod_{i=1}^{L} m_i$.

Let X and Y have RNS representations

$X \xrightarrow{RNS} (X_1, X_2, \cdots, X_L)$

$Y \xrightarrow{RNS} (Y_1, Y_2, \cdots, Y_L)$

Then

$$X \odot Y \xrightarrow{RNS} \left(\langle X_1 \odot Y_1 \rangle_{m_1}, \langle X_2 \odot Y_2 \rangle_{m_2}, \cdots, \langle X_L \odot Y_L \rangle_{m_L} \right)$$

where $\odot$ denotes addition, subtraction or multiplication.

The following statements are true for RNS systems:

1. The RNS is capable of supporting parallel, carry-free, high-speed arithmetic.
2. The RNS is an integer system that can easily support additions, subtractions and multiplications. Division is a difficult operation for the RNS.
3. The RNS is an unweighted system so comparisons are not very simple operations.

4. The RNS offers some useful properties for error detection, error correction and fault tolerance in digital systems.

- Dynamic Range of the RNS

Let M be $M = \prod_{i=1}^{L} m_i$ (M is the product of all the moduli in the moduli set).

Then, if the system supports only unsigned numbers, the Dynamic Range (DR) is

DR is $[0 \quad M-1]$.

If the system supports signed numbers the dynamic range is

$$DR = \left[-\frac{M}{2} \quad \frac{M}{2} - 1\right] \text{ if } M = \text{even}$$

$$DR = \left[-\frac{M-1}{2} \quad +\frac{M-1}{2}\right] \text{ if } M = \text{odd}$$

- RNS-to-Weighted Conversion

There are two basic techniques for converting from RNS to the weighted system. These techniques are:

- The Chinese Remainder Theorem (CRT)
- The Mixed Radix Conversion (MRC).

The Chinese Remainder Theorem technique is presented first.

(1) Chinese Remainder Theorem (CRT)

Let the moduli set be

$$S=\{m_1, m_2, \cdots, m_L\} \; ; \quad (m_i, m_j)=1 \text{ for } i \neq j$$

and let the RNS representation of X be

$$X \xrightarrow{RNS} (X_1, X_2, \cdots, X_L)$$

Then the CRT reconstructs X from its residues as shown below

$$X = \langle X_1 M_1 N_1 + X_2 M_2 N_2 + \cdots + X_L M_L N_L \rangle_M$$

or

$$X = \left\langle \sum_{i=1}^{L} X_i M_i N_i \right\rangle_M \qquad (1)$$

where $M = \prod_{i=1}^{L} m_i$; $M_i = \frac{M}{m_i}$; $N_i = \langle M_i^{-1} \rangle_{m_i}$

An alternative form of the CRT equation (1) is

$$X = \left\langle \langle X_1 N_1 \rangle_{m_1} M_1 + \langle X_2 N_2 \rangle_{m_2} M_2 + \cdots + \langle X_L N_L \rangle_{m_L} M_L \right\rangle_M$$

or

$$X = \left\langle \sum_{i=1}^{L} \langle X_i N_i \rangle_{m_i} M_i \right\rangle_M \qquad (2)$$

where again $M = \prod_{i=1}^{L} m_i$; $M_i = \frac{M}{m_i}$;

$N_i = \langle M_i^{-1} \rangle_{m_i}$.

In general, the CRT equation (2) offers more attractive implementations as compared to those offered by the CRT equat. (1).

Some examples follow:

Example 1:

Consider an RNS system defined by the set $S = \{m_1, m_2, m_3\} = \{15, 16, 17\}$; (the moduli 15, 16, 17 are pairwise relatively prime).

Here $M = \prod_{i=1}^{3} m_i = m_1 \cdot m_2 \cdot m_3 = 15 \times 16 \times 17 = 4080$.

Let the system be considered to be unsigned which means that the dyn. range is $DR = [0 \quad M-1] = [0 \quad 4079]$.

(6) d

Let X and Y be $X = 55$ and $Y = 58$ and consider performing the multiplication $Z = X \cdot Y$. The above can be done using the RNS as follows:

$$X \xrightarrow{RNS} (X_1, X_2, X_3) = (\langle X \rangle_{m_1}, \langle X \rangle_{m_2}, \langle X \rangle_{m_3})$$
$$= (\langle 55 \rangle_{15}, \langle 55 \rangle_{16}, \langle 55 \rangle_{17}) = (10, 7, 4).$$

$$Y \xrightarrow{RNS} (Y_1, Y_2, Y_3) = (\langle Y \rangle_{m_1}, \langle Y \rangle_{m_2}, \langle Y \rangle_{m_3})$$
$$= (\langle 58 \rangle_{15}, \langle 58 \rangle_{16}, \langle 58 \rangle_{17}) = (13, 10, 7).$$

Then

$$Z = X \cdot Y \xrightarrow{RNS} (Z_1, Z_2, Z_3) = (\langle X_1 \cdot Y_1 \rangle_{m_1}, \langle X_2 \cdot Y_2 \rangle_{m_2}, \langle X_3 \cdot Y_3 \rangle_{m_3})$$
$$= (\langle 10 \times 13 \rangle_{15}, \langle 7 \times 10 \rangle_{16}, \langle 4 \times 7 \rangle_{17}) = (10, 6, 11).$$

Converting $(Z_1, Z_2, Z_3) = (10, 6, 11)$ into the weighted system using the CRT one gets

$$Z = \left\langle \langle Z_1 \cdot N_1 \rangle_{m_1} \cdot M_1 + \langle Z_2 \cdot N_2 \rangle_{m_2} \cdot M_2 + \langle Z_3 \cdot N_3 \rangle_{m_3} \cdot M_3 \right\rangle_M$$

where

$$M = \prod_{i=1}^{3} m_i = 15 \times 16 \times 17 = 4080$$

$$M_1 = \frac{M}{m_1} = m_2 \times m_3 = 16 \times 17$$

(7) d

$N_1 = \langle M_1^{-1} \rangle_{m_1} = \langle (16 \times 17)^{-1} \rangle_{15} = \langle (1 \times 2)^{-1} \rangle_{15} =$

$= \langle 2^{-1} \rangle_{15} = 8$; $\left(\langle 2^{-1} \rangle_{15} = \frac{15+1}{2} = 8 \right)$.

$M_2 = \frac{M}{m_2} = m_1 \times m_3 = 15 \times 17.$

$N_2 = \langle M_2^{-1} \rangle_{m_2} = \langle (15 \times 17)^{-1} \rangle_{16} = \langle ((-1) \times 1)^{-1} \rangle_{16}$

$= \langle (-1)^{-1} \rangle_{16} = \langle -1 \rangle_{16} = 15.$

$M_3 = \frac{M}{m_3} = m_1 \times m_2 = 15 \times 16$

$N_3 = \langle M_3^{-1} \rangle_{m_3} = \langle (15 \times 16)^{-1} \rangle_{17} = \langle ((-2) \cdot (-1))^{-1} \rangle_{17} =$

$= \langle 2^{-1} \rangle_{17} = 9$; (see that $\langle 2^{-1} \rangle_{17} = \frac{17+1}{2} = 9$).

* It must be noted that if m is odd, then $\langle 2^{-1} \rangle_m = \frac{m+1}{2}$. This is due to the fact that $\langle 2 \times \frac{m+1}{2} \rangle_m = \langle m+1 \rangle_m = 1$).

The CRT then gives

$$Z = \langle \langle 10 \times 8 \rangle_{15} \times 16 \times 17 + \langle 6 \times 15 \rangle_{16} \times 15 \times 17 + \langle 11 \times 9 \rangle_{17} \times 15 \times 16 \rangle_{4080}$$

$$= \langle 5 \times 16 \times 17 + 10 \times 15 \times 17 + 14 \times 15 \times 16 \rangle_{4080} = \langle 7270 \rangle_{4080}$$

$= 3190$. Thus $\boxed{Z = X \cdot Y = 3190}$

Double check to see that $Z = X \cdot Y = 55 \times 58 = 3190$.

Example 2:

Repeat example 1 with $X=-27$ and $Y=+34$.

Here the system is signed. $M=m_1\cdot m_2\cdot m_3=4080$ and the dynamic range is $DR=\left[-\frac{4080}{2} \quad +\frac{4080}{2}-1\right]$

$=[-2040 \quad +2039]$.

$$X \xrightarrow{RNS} (X_1, X_2, X_3) = \left(\langle M-|X|\rangle_{m_1}, \langle M-|X|\rangle_{m_2}, \langle X-|X|\rangle_{m_3}\right)$$

$$= (\langle 4080-27\rangle_{15}, \langle 4080-27\rangle_{16}, \langle 4080-27\rangle_{17}) =$$

$$= (\langle 4053\rangle_{15}, \langle 4053\rangle_{16}, \langle 4053\rangle_{17}) = (3, 5, 7).$$

$$Y \xrightarrow{RNS} (Y_1, Y_2, Y_3) = (\langle Y\rangle_{m_1}, \langle Y\rangle_{m_2}, \langle Y\rangle_{m_3}) =$$

$$= (4, 2, 0).$$

Thus

$$Z = X\cdot Y \xrightarrow{RNS} (Z_1, Z_2, Z_3) = \left(\langle X_1\cdot Y_1\rangle_{m_1}, \langle X_2\cdot Y_2\rangle_{m_2}, \langle X_3\cdot Y_3\rangle_{m_3}\right)$$

$$= (12, 10, 0).$$

Converting $(Z_1, Z_2, Z_3)=(12, 10, 0)$ into the weighted system using the CRT one gets

$Z=3162$.

Recall that the system is signed with $DR = [-2040 \quad +2039]$. Since $Z = 3162 > 2039$ it means that Z is negative or

$Z = 3162 - M = 3162 - 4080 = -918$.

Double check to see that $(-27) \times (+34) = -918$

Example 3:

Repeat example 1 with $X = 55$, $Y = 84$ and consider the system to be unsigned.

Here the $DR = [0 \quad M-1] = [0 \quad 4079]$

The RNS representations of X and Y are

$X \xrightarrow{RNS} (10, 7, 4)$

$Y \xrightarrow{RNS} (9, 4, 16)$

The RNS representation of the product is

$Z = X \cdot Y \xrightarrow{RNS} (0, 12, 13)$.

Converting $(0, 12, 13)$ into the weighted system using the CRT gives

$(0, 12, 13) \xrightarrow{CRT} Z = \langle 4620 \rangle_{4080} = 540$.

Here overflow has occured. The actual

product is $X \cdot Y = 55 \times 84 = 4620$
but $4620 \notin [0 \quad 4079]$. The result we got from the RNS system is
$\langle 55 \times 84 \rangle_{4080} = 540$.

The Mixed Radix Conversion technique is presented next

② Mixed Radix Conversion (MRC) technique

Let the moduli set be
$S = \{m_1, m_2, \cdots, m_L\}$; $(m_i, m_j) = 1$ for $i \neq j$
and let the RNS representation of X be
$X \xrightarrow{RNS} (X_1, X_2, \cdots, X_L)$ where $X_1, \cdots, X_L$ are the residues. The Mixed Radix Conversion (MRC) formula is the one shown below

$$X = X_1' + m_1 \cdot X_2' + m_1 \cdot m_2 \cdot X_3' + m_1 \cdot m_2 \cdot m_3 \cdot X_4' + \cdots$$
$$+ \cdots + m_1 \cdot m_2 \cdot m_3 \cdots m_{L-1} \cdot X_L' \qquad (3)$$

where $X_1', X_2', \cdots, X_L'$ are called the mixed radix digits and $X_i' \in Z_{m_i}$.

The mixed radix digits $X_1', X_2', \cdots, X_L'$ can be expressed as functions of the residues $X_1, \cdots, X_L$ and the moduli $m_1, \cdots, m_L$.

The MRC formula of equation (3) represents a weighted system. The mixed radix digits $X_1', X_2', \cdots, X_L'$ have weights associated to them. The weight associated to X_1' is 1, the weight associated to X_2' is m_1, the weight associated to X_3' is $m_1 \times m_2$, $\cdots$, the weight associated to X_L' is $m_1 \times m_2 \times m_3 \times \cdots \times m_{L-1}$. Thus, X_1' is the least significant mixed radix digit while X_L' is the most significant mixed radix digit. Obviously, comparisons between two numbers X and Y can easily be performed by comparing their mixed radix digit representations $(X_1', X_2', \cdots, X_L')$ and $(Y_1', Y_2', \cdots, Y_L')$.

It will now be shown how the mixed radix digits can be expressed as functions of the residues and the moduli. The procedure will be shown for a 4-moduli system

but it can easily be generalized to any arbitrary L-moduli system.

Consider a 4-moduli RNS system based on the moduli set $S=\{m_1, m_2, m_3, m_4\}$ and let the RNS representation of X be $X \xrightarrow{RNS} (X_1, X_2, X_3, X_4)$ where X_1, X_2, X_3, X_4 are the residues. The Mixed radix conversion (MRC) formula is

$$X = X_1' + m_1 \cdot X_2' + m_1 \cdot m_2 \cdot X_3' + m_1 \cdot m_2 \cdot m_3 \cdot X_4' \quad (4)$$

Taking mod m_1 both sides of eq. (4) yields

$$\langle X \rangle_{m_1} = \langle X_1' \rangle_{m_1} = X_1' \; ; \; (\langle X_1' \rangle_{m_1} = X_1' \text{ since } X_1' \in Z_{m_1}).$$

Due to the fact that $\langle X \rangle_{m_1} = X_1$ one gets

$$\boxed{X_1' = X_1} \quad (5).$$

Starting again from equation (4) we get

$$X - X_1' = m_1 X_2' + m_1 \cdot m_2 X_3' + m_1 \cdot m_2 \cdot m_3 \cdot X_4'$$

or

$$m_1^{-1}(X - X_1') = X_2' + m_2 X_3' + m_2 m_3 X_4'$$

or

$$\langle m_1^{-1}(X - X_1') \rangle_{m_2} = \langle X_2' \rangle_{m_2} = X_2'$$

or

$$\boxed{X_2' = \langle m_1^{-1}(X_2 - X_1') \rangle_{m_2}} \qquad (6)$$

Regarding the computation of X_3' equation (4) gives

$$X - X_1' - m_1 X_2' = m_1 m_2 X_3' + m_1 m_2 m_3 X_4'$$

or

$$(m_1 m_2)^{-1} \cdot (X - X_1' - m_1 X_2') = X_3' + m_3 X_4'$$

or

$$\langle (m_1 m_2)^{-1} \cdot (X - X_1' - m_1 X_2') \rangle_{m_3} = \langle X_3' \rangle_{m_3} = X_3'$$

Thus

$$\boxed{X_3' = \langle (m_1 m_2)^{-1} \cdot (X_3 - X_1' - m_1 X_2') \rangle_{m_3}} \qquad (7)$$

Finally, regarding the computation of X_4' equation (4) gives

$$X - X_1' - m_1 X_2' - m_1 m_2 X_3' = m_1 m_2 m_3 X_4'$$

or

$$(m_1 m_2 m_3)^{-1} \cdot (X - X_1' - m_1 X_2' - m_1 m_2 X_3') = X_4'$$

or

$$\langle (m_1 m_2 m_3)^{-1} (X - X_1' - m_1 X_2' - m_1 m_2 X_3') \rangle_{m_4} =$$

$$= \langle X_4' \rangle_{m_4} = X_4'$$

Thus

$$\boxed{X_4' = \langle (m_1 m_2 m_3)^{-1} (X_4 - X_1' - m_1 X_2' - m_1 m_2 X_3') \rangle_{m_4}} \quad (8)$$

Equations (5)–(8) show expressions of the mixed radix digits as functions of the residues and the moduli.

An example follows:

Example 4: Consider an RNS system defined by the moduli set $S = \{m_1, m_2, m_3, m_4\} = \{7, 9, 11, 13\}$. Let the RNS representation

of a number X be

$$X \xrightarrow{RNS} (X_1, X_2, X_3, X_4) = (1, 2, 4, 9).$$

Convert the number X into its weighted form using the MRC technique.

Answer: The mixed radix digits are obtained from equations (5)–(8). These equations give

$$X_1' = 1; \quad X_2' = 4; \quad X_3' = 1; \quad X_4' = 2.$$

The MRC formula of equation (4) then gives $X = 1478$.

Question: So what is so good about RNS?

Answer: Consider an RNS based on set $S = \{m_1, m_2, \cdots, m_{14}\} = \{19, 23, 29, 31, 37, 41, 43, 47, 53, 55, 59, 61, 63, 2^6 = 64\}$. The moduli m_i of set S are pairwise relatively prime while $\prod_{i=1}^{14} m_i \cong 2^{75}$. The dynamic range achieved by an RNS system based on set S is approximately 75 bits. The largest modulus in set S (which dictates the speed of the internal RNS processing) is $64 = 2^6$. But $\langle X \rangle_{2^6} \leq 2^6 - 1$ while $2^6 - 1$ can be represented by six bits. Thus, although the entire RNS system can perform 75-bit computations, (DR $\cong$ 75 bits), it can perform them at the speed of 6-bit processing hardware.

As another example consider an RNS based on set

$$R = \{m_1, m_2, \cdots, m_7\} = \{2^{12}+1, 2^{13}-1, 2^{14}+1, 2^{15}-1, 2^{16}+1, 2^{17}-1, 2^{17}\}.$$

The seven moduli of set R are pairwise relatively prime while $\prod_{i=1}^{7} m_i \cong 2^{104}$ and the system's dynamic range is DR ≅ 104 bits. The slowest channel is the channel mod 2^{17} which relies on 17-bit processing hardware. Also, all the moduli of set R are attractive forms 2^a-1, 2^b+1, 2^c. These moduli forms imply simple weighted-to-RNS and RNS-to-weighted conversions as well as simple and efficient RNS arithmetic.

Question: Is RNS a good choice of a system in order to perform one computation? (say $c = a \odot b$ where $\odot = +, -, \times$?).

Answer: No it is not. This is due to the fact that the time involved for converting a and b from the weighted system into the RNS and the time involved for converting the result $c = a \odot b$ from the RNS back to the weighted system will take away all the speed benefits implied

by the fast internal RNS processing.

Question: When is RNS a good choice of a computing system?

Answer: RNS is an excellent choice in case of computationally intensive environments. This means problems which rely on large number of computations (a lot of processing) and relatively small number of conversions from the weighted system to the RNS and from the RNS to weighted.

Consider for example two polynomials in x ; $P(x) = \sum_{i=0}^{999} a_i x^i$ and $Q(x) = \sum_{i=0}^{999} b_i x^i$ and consider computing their product $R(x) = P(x)\,Q(x) = \sum_{i=0}^{1998} c_i x^i$. The inputs to this computation are the 2,000 data points (coefficients) $\{a_0, a_1, \cdots, a_{999}\}$; $\{b_0, b_1, \cdots, b_{999}\}$.

The produced results are the 1999 coefficients of $R(x)$ or the sequence $\{c_0, c_1, \cdots, c_{1998}\}$. The computational requirement is 10^6 multiplications and $(999)^2 \cong 10^6$ additions.

It must be mentioned that polynomial products $P(x)Q(x)$ are very useful because they realize many useful Digital Signal Processing (DSP) computations like the linear convolution which is the heart of linear filtering etc.

Problem:

Consider an RNS system with moduli set $S=\{m_1, m_2, m_3\}$.

(a) Let two numbers X and Y be represented in the RNS domain as

$$X \xrightarrow{RNS} (X_1, X_2, X_3) = (10, 4, 15)$$
$$Y \xrightarrow{RNS} (Y_1, Y_2, Y_3) = (12, 8, 4)$$

Which is the largest number between X and Y?

(20) d

(b) Consider two numbers X and Y with mixed radix digits $(X_1', X_2', X_3') = (1, 4, 20)$ and $(Y_1', Y_2', Y_3') = (5, 10, 13)$. Here X_1' and Y_1' are the least significant mixed radix digits of X and Y while X_3' and Y_3' are the most significant mixed radix digits of X and Y.

Which is the largest number between X and Y?

Answer:

(a) We can not compare. RNS is unweighted

(b) Here $X > Y$ since its most significant mixed radix digit X_3' is larger then the most significant mixed radix digit Y_3' of the # Y.