MODULE II

More Number Theory and Some Algebra; Z_n (Z mod n)

As we already know $(Z, +, \circ)$ has "algebraic" structure.
Indeed. both + and $\circ$ are binary operations on Z that are associative and commutative; 0 is the identity of $(Z, +)$, 1 is the identity of $(Z,\circ)$ and the operations are linked by the distributive law $a \circ (b + c) = a \circ b + a \circ c$.
We put these ideas in a more general context and begin a discussion of Z_n, the integers module n, in this algebraic setting.

Definition 1 A binary operation $*$ on a non-empty set S is a function $*$: $S \times S \to S$. The operation * is said to be associative if

$$\forall a, b, c \in S \quad (a * b) * c = a * (b * c))$$

If $*$ is associative then $(S,*)$ is called a semigroup. An element e is called an identity provided $\quad a * e = e * a = a \qquad \forall a \in S$.

If an identity exists it is unique (indeed $e_1 = e_1 \cdot e_2 = e_2$) and $(S,*)$ is referred to as a monoid. An element a is said to be invertible (or to have an inverse) if $\exists$ b such that

$$a * b = b * a = e$$

If an inverse exists it is unique (Proof - Exercise 1) and is denoted by a^{-1}. If all elements of the monoid $(S,*)$ are invertible then $(S,*)$ is a group

(Exercise 2: If $T = \{a \in S \mid a \text{ has an inverse}\}$ then $(T,*)$ is a group).

If $*$ is commutative, i.e. $\forall a, b \in S \ (a * b = b * a)$
$(S,*)$ is referred to as a commutative semigroup or commutative monoid or commutative group as the case may be. If the operation is denoted by + and $(S, +)$ is a commutative group it is usually referred to as an abelian group.

If the non-empty set R is equipped with two binary operations + and $\circ$, the triple $(R, +, \circ)$ is called a ring if

(i) $(R, +)$ is an abelian group with identity 0 (inverses are denoted with minus signs, i.e. the inverse of a has the name -a)

(ii) $(R, \circ)$ is a semigroup

and

(iii) (distributive laws) $\forall$ a, b, c $\in$ R

$$a \circ (b + c) = a \circ b + a \circ c$$

and

$$(b + c) \circ a = b \circ a + c \circ a$$

Exercise 3. (Submit this one) If $(R, +, \circ)$ is a ring then $\forall\, a \in R$

$$a \circ 0 = 0 \circ a = 0$$

Thus if $(R,\circ)$ has an identity, say 1, and $|R| \geq 2$ then $1 \neq 0$

Prove these contentions.

If $|R| \geq 2$ and $(R,\circ)$ is a monoid, then $(R, +, \circ)$ is a ring with identity.

An element $a \in R$, where $(R, +, \circ)$ is a ring with identity, is called a unit if it has a multiplicative inverse. The set of units $U \subseteq R - \{0\}$ and $(U, \circ)$ is a group. It is called the group of units of R.

Exercise 4. Prove $0 \notin U$ and $(U,\circ)$ is group

If $(R,\circ)$ is a commutative semigroup then $(R, +, \circ)$ is called a commutative ring.

A commutative ring with identity such that $U = R - \{0\}$ is a field.

Remark1. $(Z, +, \circ)$ is a commutative ring with identity such that $U = \{1, -1\}$.

Definition 2. Let $n \in Z^+$. We write $a \equiv b \pmod{n}$ if and only if $n \mid a-b$

Terminology: a is congruent to b modulo n

Observation Congruence modulo n is an equivalence relation. Each equivalence class contains a unique element from $\{0, 1, \ldots, n-1\}$ called the least residue of the class and is determined by the division algorithm, i.e. the least residue of the equivalence class containing a is given by r where $a = q\,n + r$ and $0 \leq r \leq n-1$.

Thus there is exactly one equivalence class for each $0 \leq r \leq n-1$ and we use these numbers to represent the equivalence classes.

Definition 3. $Z_n = \{0, 1, \ldots, n-1\}$ the integers modulo n, is the collection of equivalence classes referred to above.

Also $\quad a +_n b \triangleq c$

where $\quad a + b \equiv c \pmod{n}$

and $\quad a \circ_n b \triangleq d$

where $\quad a \circ b \equiv d \pmod{n}$

Example 1. $Z_{36} = \{0, 1, 2, \ldots, 35\}$

$$24 +_{36} 25 = 13$$

$$9 \circ_{36} 8 = 0$$

Exercise 5. (Submit a and b)

a) Let $a, b, c, d \in Z$ and $n \in Z^+$. Prove

i) $a \equiv b \pmod{n} \Leftrightarrow b \equiv a \pmod{n} \Leftrightarrow a - b \equiv 0 \pmod{n}$

ii) $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

iii) $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n} \Rightarrow a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$

iv) $a \equiv b \pmod{n}$ and $d \mid n \Rightarrow a \equiv b \pmod{d}$

v) $a \equiv b \pmod{n}$ and $c > 0 \Rightarrow ac \equiv bc \pmod{cn}$

Remark 2 i) and ii) verify symmetry and transitivity of the equivalence relation:

a is related to b if and only if $a \equiv b \pmod{n}$

iii) verifies that $+_n$ and $\circ_n$ are well-defined

b) Prove i) $ax \equiv ay \pmod{n} \Leftrightarrow x \equiv y \left(\bmod \dfrac{n}{\gcd(a,n)}\right)$

ii) $ax \equiv ay \pmod{n}$ and $\gcd(a,n) = 1 \Rightarrow x \equiv y \pmod{n}$

iii) $x \equiv y \pmod{n_i}$ $i = 1,.., k \Leftrightarrow x \equiv y \pmod{\ell cm(n_1,.., n_k)}$

iv) if $n_1,.., n_k$ are pairwise relatively prime then $x \equiv y \pmod{n_i}$ $i = 1,.., k$

$$\Leftrightarrow x \equiv y \left(\bmod \prod_{i=1}^{k} n_i\right)$$

c) Prove: if $b \equiv c \pmod{n}$ then $\gcd(b, n) = \gcd(c, n)$

d) Prove: if p is prime and $a^2 \equiv b^2 \pmod{p}$ then $p \mid (a+b)$ or $p \mid (a-b)$

e) Suppose f(x) is a polynomial with integer coefficients.

Prove: If $f(a) \equiv k \pmod{n}$ then $f(a + tn) \equiv k \pmod{n}$ $\forall$ integers t.

Remark 3. Even though the notation used in the preceding discussion and exercise is rather standard it tends to obfuscate the essential nature of the operations. In actuality the operations are very simple to describe. Indeed, we leave it to the reader to show that $+_n$ and $\circ_n$ can be defined as follows: if $a, b \in Z$ and $\bar{a}, \bar{b}$ represent the equivalence classes containing a and b respectively then

$$\bar{a} +_n \bar{b} = \overline{a+b}$$

and

$$\bar{a} \circ_n \bar{b} = \overline{ab}$$

In some of the discussions to follow we drop the subscript "n" on the operations and simply use + and $\circ$ to denote modulo n arithmetic.

Proposition 1 $(Z_n, +, \circ)$ is a commutative ring with identity. The elements 0 and 1 are the respective identities of $(Z, +)$ and $(Z, \circ)$. The group of units is denoted by Z_n^*.

Remark 5. We shall not prove this proposition as it is straight – forward and TEDIOUS.

Proposition 2. $Z_n^* = \{a \in Z_n \mid \gcd(a,n) = = 1\}$

Pr oof Suppose $a \in Z_n^*$ so that $a \cdot a^{-1} = 1$ i.e. $aa^{-1} \equiv 1 \pmod n$

Thus $\quad a\,a^{-1} = q\,n + 1$

so if $k \mid a, n$ it follows that $k \mid 1$, i.e. $\gcd(a, n) = 1$

Conversely, suppose $\gcd(a, n) = 1$. Then $\exists\, x, y \in Z$ such that

$$a\,x + n\,y = 1$$

or $\quad a\,x \equiv 1 + (-y)n.$

Hence $\quad a\,x \equiv 1 \pmod n$.

Choose $b \in \{0, 1,.., n\text{-}1\}$ such that $b \equiv x \pmod n$

Then $a\,b \equiv a\,x \equiv 1 \pmod n$ i.e. $= 1$ in Z_n

Corollary 2.1 $|Z_n^*| = \varphi(n)$

Corollary 2.2 If p is prime then $Z_p^* = Z_p - \{0\}$, so Z_p is a field. Furthermore, if Z_n is a field then n is prime.

Exercise 6 (Submit b.)

a) Determine Z_{30}^*

b) Prove the following generalization of the previous proposition:

Let $d = \gcd(a, n)$. Then $\exists\, x \in Z_n, \cdot\cdot$ a solution of $a\,x \equiv b \pmod n$, if and only if $d \mid b$. In this case there are exactly d solutions in Z_n and they are all congruent modulo n/d.

Example 2. In Z_9, $Z_9^* = \{1, 2, 4, 5, 7, 8\}$ where

$1^{-1} = 1$

$2^{-1} = 5$ (because $2.5 = 10 \equiv 1 \pmod 9$)

$4^{-1} = 7$ (because $4.7 = 28 \equiv 1 \pmod 9$)

$8^{-1} = 8$ (because $8.8 = 64 \equiv 1 \pmod 9$

Consider the equation

$$3x \equiv b \pmod 9$$

If b = 0 then solutions are 0, 3, 6 (which are congruent mod 3)

If b = 3 the solutions are 1, 4, 7 (which are congruent mod 3)

If b = 6 the solutions are 2, 5, 8 (which are congruent mod 3)

No solutions exist otherwise, i.e. for $b \in Z_9$, $b \neq 0, 3, 6$.

In the proof of the multiplicativity of the Euler-phi- function φ we established a special case of our next theorem, the important Chinese Remainder Theorem. We prove the theorem by using the so-called Gauss algorithm for computing the solution. It is actually an explicit formula for the solution which becomes intuitively appealing upon some inspection.

Theorem 1. Let $n_1, n_2, .., n_k \in Z^+$ be pairwise relatively prime. Then the system of simultaneous congruences

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\bullet$$
$$\bullet$$
$$\bullet$$
$$x \equiv a_k \pmod{n_k}$$

has a UNIQUE solution modulo $n = n_1 n_2 \bullet\bullet\bullet n_k$ (i.e. in Z_n)

Proof First we prove existence. Let $\hat{x} = \sum_{i=1}^k a_i \left(\frac{n}{n_i}\right) M_i$

where $M_i \equiv \left(\frac{n}{n_i}\right)^{-1} \bmod n_i$, $i = 1,.., k$. Observe that $\left(\frac{n}{n_i}\right)^{-1}$ exists

in Z_{n_i} because n_i and $\frac{n}{n_i}$ are relatively prime. Also

$$a_i \frac{n}{n_i} M_i \equiv a_i \pmod{n_i}$$

because $\frac{n}{n_i} M_i \equiv 1 \pmod{n_i}$. Moreover

$$a_j \left(\frac{n}{n_j}\right) M_j \equiv 0 \pmod{n_i} \text{ for } j \neq i$$

because $n_i \mid \left(\frac{n}{n_j}\right)$. Thus

$$\hat{x} = \sum_{j=1}^k a_j \left(\frac{n}{n_j}\right) M_j$$
$$\equiv a_i \pmod{n_i} \text{ for each } i = 1, 2.., n.$$

Let $x \in Z_n$ such that $\hat{x} \equiv x \pmod{n}$

Because $n_i \mid n$,

$$x \equiv a_i \bmod n_i \text{ for each } i = 1,..,k$$

so setting $x = \hat{x} \bmod n$ we obtain a solution in Z_n.

As for uniqueness suppose x_1 and x_2 are solutions and $x_1, x_2 \in Z_n$.

Then, assuming $x_1 \geq x_2$

$$x_1 - x_2 \equiv a_i - a_i = 0 \pmod{n_i}$$

Thus $\quad n_i \mid x_1 - x_2 \qquad i = 1,.., k$

But then $n = n_1 ... n_k \mid x_1 - x_2$ because $n_1, n_2,.., n_k$ are pairwise relatively prime.

Finally then $x_1 - x_2 = 0$ because $0 \leq x_2 \leq x_1 \leq n-1$.

<u>Example 3</u>. Consider $n_1 = 7, n_2 = 13, n_3 = 15$ and

$$x \equiv 3 \pmod{7}$$
$$x \equiv 7 \pmod{13}$$
$$x \equiv 13 \pmod{15}$$

Then $\quad n = (7)(13)(15) = 1365$

$$\frac{n}{n_1} = 195, \ M_1 = (195)^{-1} \bmod 7$$
$$= (6)^{-1} \bmod 7 = 6$$

$$\frac{n}{n_2} = 105, \ M_2 = (105)^{-1} \bmod 13$$
$$= (1)^{-1} \bmod 13 = 1$$

$$\frac{n}{n_3} = 91, \ M_3 = (91)^{-1} \bmod 15$$
$$= (1)^{-1} \bmod 15 = 1$$

Thus

$$\hat{x} = (3)(195)(6) + (7(105)(1) + (13)(91)(1)$$
$$= 1560 + 735 + 1183$$
$$= 5428$$

so $\quad \underline{\underline{x}} = \underline{\underline{1333}}$

Check: $\quad 1333 = (190)(7) + \underline{3}$

$1333 = (102)(13) + \underline{7}$

$1333 = (88)(15) + \underline{13}$

Exercise 7. Solve $x \equiv 3 \pmod 5$

$x \equiv 3 \pmod 7$

$x \equiv 5 \pmod{12}$

for the unique solution in Z_{420}.

Remark 6. Of course this explicit expression for the solution provides for a convenient algorithmic computational procedure given algorithms for computing the terms in the expressions. The only computational procedure that deserves mention is that of computing inverses modulo n.

Modulo n Inverse Algorithm

Input: $a \in Z_n$

Output: a^{-1} modn, provided it exists

1. Apply the extended Euclidean algorithm to find (d, x, y) such that
   $d = \gcd(x, y)$ and $d = a\,x + n\,y$
2. If $d > 1$ then a^{-1} modn doesn't exist. Otherwise apply the Division Algorithm and return (x modn).

Exercise 8. Write an algorithm for the solution of the system of simutaneous congruences given pairwise relatively prime $n_1, n_2, .., n_k$ and elements $a_i \in Z_{n_i}$ $i = 1,.., k$. What is its complexity?

Remark 7. We noted that $\varphi(n) = \left|Z_n^*\right|$ so that Z_n^* is a FINITE group. Before examining Z_n^* in more detail we discuss some generalities regarding finite groups.

Definition(s) 4. Let $(G,*)$ be a finite group. The order of G is just $|G|$. If $H \subseteq G$ and the restriction of $*$ to H renders $(H,*)$ a group then H is called a subgroup of G, denoted by $H \subseteq_g G$ (This is the case even if $|G| = \infty$).

<u>Proposition 3</u>. Let $(G,*)$ be a group.

i) $H \subseteq_g G$ if and only if $\forall\, a, b \in G(a, b \in H \Rightarrow a\, b^{-1} \in H)$

ii) $|G| < \infty$ and $H \subseteq_g G \Rightarrow |H| \mid |G|$

iii) $|G| < \infty$ and $a \in G \Rightarrow \exists\, n \in Z^{+}$ such that $a^{n} = c$

The smallest such n is called the <u>order of a</u>, denoted ord(a)

and $(a) \underline{\underline{\Delta}} \{a^{k} \mid k \geq 1\} \subseteq_g G$ such that $|(a)| = \text{ord}(a)$.

Thus $\text{ord}(a) \mid |G|$ and so $a^{|G|} = e$ as well. Furthermore, if $a^{k} = e$ then $\text{ord}(a) \mid k$.

iv) if $a, b \in G$, a finite group, such that $a\, b = b\, a$

and

$$\gcd(\text{ord } a, \text{ord } b) = 1$$

then

$$\text{ord}(a\, b) = \text{ord}(a) \bullet \text{ord}(b)$$

In fact, if $a_1, .., a_k \in G$ commute in pairs and ord $a_1, .., $ ord a_k are pairwise relatively prime then $\text{ord}(a_1 \bullet\bullet\bullet\, a_k) = (\text{ord } a_1) \bullet\bullet\bullet (\text{ord } a_k)$

<u>Proof</u> (i) $(\Rightarrow)$: Let e_H denote the identity of H. Then $e_H = e_H \cdot e_H$. But e_H^{-1} exists in G so

$$e = e_H^{-1} * e_H = e_H^{-1} * (e_H * e_H) = (e_H^{-1} * e_H) * e_H = e_H,$$ i.e. the identity of G is also the identity of H. But then uniqueness of inverse implies that the inverse of an element of H in G is the inverse in H. Hence $a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow a * b^{-1} \in H$.

$(\Leftarrow)$: First choose $a \in H$ so $a, a \in H$ and therefore, $e = a * a^{-1} \in H$.

Hence $b \in H$ implies $e, b \in H$ which implies $b^{-1} = e * b^{-1} \in H$.

Next $a, b \in H$ implies $a, b^{-1} \in H$ which implies $a * b = a * \left(b^{-1}\right)^{-1} \in H$

Since $*$ is associative on H we have that $H \subseteq_g G$.

(ii) Define a Rb if and only if $aH = bH$ $\left(\text{where } a H \underline{\underline{\Delta}} \{a * h \mid h \in H\}\right)$.

It is the case that R is an equivalence relation on G; we only verify that $aH = \{a h \mid h \in H\}$ is the equivalence class containing a:

- $a \in aH$ because $a = a * e$ and $e \in H$
- $bR a$ if and only if $b \in aH$ - indeed if $b \in aH$

i.e. $b = a * h$ for some h, then $b * \hat{h} = a * \left(h * \hat{h}\right) \in aH \ \forall \ \hat{h}$ so $bH \subseteq aH$.

Likewise $a = b * h^{-1} \in bH$ so $aH \subseteq bH$ and so a R b. Conversely, if $aH = bH$ then $b = b * e \in bH = aH$.

Next observe that $|H| = |bH| \ \forall \ b \in G$

since $\begin{array}{l} H \to bH \\ h \to bh \end{array}$ is easily seen to be

a bijection. Thus G, being the pairwise disjoint union of equal size equivalence classes of common size $|H|$, has order which is divisible by $|H|$.

(iii) Since $(a) = \{a^k \mid k \geq 1\} \subseteq G$, (a) is finite.

Thus $\exists \ 1 \leq \ell < k$ such that $a^k = a^\ell$. But $a^{-\ell} = \left(a^{-1}\right)^\ell$ so $a^k * \left(a^{-1}\right)^\ell = \left(a^\ell\right) * \left(a^{-1}\right)^\ell = e$.

Hence $a^{k-\ell} = e$ and $k - \ell > 0$.

Let m be the smallest positive integer such that $a^m = e$

By the division algorithm $(a) = \{c, a, \ldots, a^{m-1}\}$ so, it being clear that $(a) \subseteq_g G$,

$$m = |(a)| \ \Big| \ |G|$$

Of course if $a^k = e$ then, by the Division Algorithm, $k = q\,m + r$ such that $0 \leq r \leq m-1$ and

$$e = a^k = \left(a^m\right)^q a^r = a^r$$

But $r < m$ forces $r = 0$ and so $m \mid k$.

(iv) Realize to begin with that, by induction, $(a\,b)^t = a^t b^t$ $\forall\, t \geq 1$. Thus

$$e = (a\,b)^{\text{ord}(a\,b)\,\text{ord}(b)}$$
$$= a^{\text{ord}(a\,b)\,\text{ord}(b)}\ \ b^{\text{ord}(b)\ \text{ord}(a\,b)}$$
$$= a^{\text{ord}(a\,b)\cdot\,\text{ord}(b)}$$

and so, by (iii)

$$\text{ord}(a) \mid \text{ord}(a\,b)\cdot\ \text{ord}(b)$$

But gcd(ord(a), ord(b)) = 1 forces

$$\text{ord}(a) \mid \text{ord}(a\,b)$$

Likewise

$$\text{ord}(b) \mid \text{ord}(ab)$$

and because gcd(ord(a), ord(b) = 1, it follows that $(\text{ord}(a))\,(\text{ord}(b)) \mid \text{ord}(ab)$.

Of course

$$(a\,b)^{\text{ord}(a)\,\text{ord}(b)}$$
$$= \quad a^{\text{ord}(a)\cdot\,\text{ord}(b)} \cdot b^{\text{ord}(b)\cdot\,\text{ord}(a)}$$
$$= \quad e \cdot e = e$$

and, again by (iii), $\text{ord}(a\,b) \mid \text{ord}(a)\cdot\ \text{ord}(b)$.

The result for arbitrary k follows by induction

<u>Exercise 9</u>. Prove (iv) for arbitrary $k \geq 2$.

<u>Exercise 10</u>. (Submit c)

a) Let m be a negative integer. Define $a^m \underline{\underline{\Delta}} (a^{-1})^{|m|}$

for $a \in G$ (a group). Prove: $\forall\, m, n \in Z \quad \forall a \in G\ a^{m+n} = a^m * a^n$

and $(a^m)^n = a^{mn}$.

Recall: $a^k \underline{\underline{\Delta}}\, a \cdot a^{k-1} \quad \forall\, k \geq 1$ and $a^o \underline{\underline{\Delta}}\, e$

b) Prove: $\text{ord}(a^{-1}) = \text{ord}(a)$ for each $a \in G$(a finite group)

c) Determine the orders of the elements of Z_{30}^*.

<u>Corollary 3.1</u> a) (Euler's theorem) If $a \in Z_n^*$, $n \geq 2$, then

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

b) If $a \in Z_n^*$, $\text{ord}(a) = m$ and $a^k \equiv 1 \pmod n$

then $m | k$. In particular $m | \varphi(n)$.

<u>Proof</u> We need only note that $\left|Z_n^*\right| = \varphi(n)$ and 1 is the identity of Z_n^*.

Remark 8. A special case of Corollary 3.1a) yields

Fermat's theorem: if p is prime and $\gcd(a, p) = 1$ then $a^{p-1} \equiv 1 \bmod p$. Indeed, by the Division Algorithm, $\exists\, r \in Z_p$ such that $a \equiv r \bmod p$ and $r \neq 0$. But, as previously noted in Corollary 2.2, $Z_p - \{0\}$, is a group, i.e.

$Z_p - \{0\} = Z_p^*$ and so

$$r^{p-1} \equiv 1 \bmod p$$

Thus $\quad a^{p-1} \equiv 1 \bmod p$

since $\quad a^{p-1} \equiv r^{p-1} \bmod p$.

Also note that $a^p \equiv a \bmod p \quad \forall\, a$.

Another important result on congruences which generalizes Euler's theorem is given next.

Proposition 4. If n is a product of distinct primes and r, s > 0 then

$\forall\, a \in Z \ \left(r \equiv s(\bmod\ \varphi(n)\right) \Rightarrow\ a^r \equiv a^s\ (\bmod\ n))$

In particular if $n = p$ a prime, then $\forall a(r \equiv s\ (\bmod\ (p-1))$

$\Rightarrow\ a^r \equiv a^s \bmod p.)$.

Proof First observe that we may assume $a \in Z_n$ and that $a \neq 0$. Indeed if $a \notin Z_n$ then $\exists\, b \in Z_n$ such that $a \equiv b \bmod n$. But then $a^k \equiv b^k \bmod n\ \forall\, k$.
If $a = 0$ the result is trivially true.

Now suppose $a \in Z_n^*$ so that $a^{\varphi(n)} \equiv 1\ (\bmod\ n)$.

But $\quad r = q\ \varphi(n) + s$

so $\quad a^r = (a^{\varphi(n)})^q \cdot a^s$

Since $\quad a^{\varphi(n)} \equiv 1 \bmod n, \quad a^r \equiv a^s (\bmod\ n)$

Suppose $a \notin Z_n^*$ so that $\gcd(a, n) = d > 1$

Now $n = n'd$, $a = a'd$ where $\gcd(n', a') = 1$. Also, since n is a product of distinct primes $\gcd(n', d) = 1$ so $\varphi(n) = \varphi(n')\ \varphi(d)$. As $r \equiv s\ (\bmod\ \varphi(n))$ we may write $r - s = \alpha\ \varphi(n')\ \varphi(d)$ for some $\alpha \in Z$. Consider

$$\begin{aligned} a^{r-s} &= (a')^{r-s}\ (d)^{r-s} \\ &= (a')^{\varphi(n')\,\varphi(d)\alpha}\ (d)^{\varphi(n')\,\varphi(d)\alpha} \end{aligned}$$

But $\gcd(a', n') = 1 \Rightarrow (a')^{\varphi(n')} \equiv 1 \pmod{n'}$ which, in turn, forces

$$(a')^{\varphi(n')\varphi(d)\alpha} \equiv 1 \pmod{n'}$$

Likewise $\gcd(d, n') = 1 \Rightarrow (d)^{\varphi(n')} \equiv 1 \pmod{n'}$

and so

$$(d)^{\varphi(n')\varphi(d)\alpha} \equiv 1 \pmod{n'}$$

Thus

$$a^{r-s} \equiv 1 \pmod{n'}$$

so

$$a^r \equiv a^s \pmod{n'}$$

follows.

As $r, s > 0$ we see that $d \mid a \Rightarrow d \mid a^r - a^s$

Now

$$n' \mid a^r - a^s \qquad \text{and} \qquad d \mid a^r - a^s$$

together with $\gcd(n', d) = 1$ forces $n = n'd \mid a^r - a^s$ i.e. $a^r \equiv a^s \pmod{n}$.

<u>Remark 9</u>. If $r > 0$, $s = 0$ (or $r = 0$, $s > 0$) the result is <u>not</u> true.

<u>Example 4</u>. Let $n = 6$ so $\varphi(6) = 2$. Set $r = 2$ so $r \equiv 0 \pmod{2}$. Note for $a = 4 \notin Z_6^*$

$$a^r = 4^2 = 16 \equiv 4 \bmod 6 \neq 1 \bmod 6.$$

Of course, it is the case that

$$r \equiv 0 \pmod{\varphi(n)} \Rightarrow a^r \equiv 1 \pmod{n} \text{ for } \underline{\underline{\underline{a \in Z_n^*}}}$$

<u>Remark 10</u>. If one wants to raise an integer a to a power modulo n and the power is not congruent to 0 modulo $\varphi(n)$ then the computation may be done with a power which is congruent to the original power modulo $\varphi(n)$ (Here n is a product of <u>distinct</u> primes).

Example 5. Consider n= (2) (3) (5) = 30, a = 63 and r = 10. We desire the value of $63^{10} \pmod{30}$.

First $63 \equiv 3 \pmod{30}$

so $63^{10} \equiv 3^{10} \pmod{30}$

Now $\varphi(30) = 8$

and $10 \equiv 2 \pmod{8}$

so $3^{10} \equiv 3^2 \pmod{30}$

and, finally, $63^{10} \equiv 9 \pmod{30}$

On the other hand consider r = 8 (= 0 mod $\varphi(30)$)

Then $63^8 \equiv 6561 \equiv 21 \pmod{30} \not\equiv 1 \pmod{30}$

Finally consider $a = 7 \in Z_{30}^*$ and r = 8; then

$$7^8 = 1443001 \equiv 1 \bmod 30.$$

Exercise 11. Let $n = 4 = 2^2$ and a = 2 and r = 3, s = 1

Calculate: a^s and a^r mod 4. Does $a^r = a^s \pmod{n}$? What does this say about the advisability of dropping the condition that n be a product of distinct primes in the previous result?

An algorithm for modular exponentiation is given next; but first an observation:

Observation If $k = \sum_{i=0}^{t} k_i 2^i$ ($k_i = 0, 1$) is the binary representation of k then

$$a^k = (a^{2^0})^{k_0} (a^{2^1})^{k_1} \cdots (a^{2^t})^{k_t}$$

Algorithm (Repeated Square -and-Multiply)

Input: $a \in Z_n$ and $k = \sum_{i=0}^{t} k_i 2^i$

Output: a^k mod n

1. Set $b \leftarrow 1$; if k = 0 return (b)
2. Set $A \leftarrow a$
3. If $k_0 = 1$ then set $b \leftarrow a$
4. For i = 1,..., t do the following:
    4.1 Set $A \leftarrow A^2 \bmod n$
    4.2 If $k_i = 1$ set $b \leftarrow A \cdot b \bmod n$
5. Return (b)

Example 6. Evaluate 4^{35} mod 30

Input: $a = 4,\ k = 1\cdot 2^0 + 1\cdot 2^1 + 0\cdot 2^2 + \cdot 02^3 + 02^4 + 1\cdot 2^5$

Steps 1. b = 1

2. A = 4

3. Since $k_0 = 1$, b = 4

4's. i) i = 1 4.1 A = 16 mod 30 = 16

4.2 b = (16) 4 mod 30 = 4

ii) i = 2 4.1 A = 256 mod 30 = 16

iii) i = 3 4.1 A = 256 mod 30 = 16

iv) i = 4 4.1 A = 256 mod 30 = 16

v) i = 5 4.1 A = 256 mod 30 = 16

4.2 b = (16)(4) mod 30 = 4

5. b = 4

Check : n = 30 $\varphi(n) = 8$, 35 = 3 mod 8 so $4^{35} = 4^3$ mod 30 = 4 mod 30.

Exercise 12. (Submit a) a) evaluate 5^{75} mod 35 using the algorithm. Can you check this using the previous theorem? If so do so.

b) If k < n then the algorithmic complexity is $O((1gn)^3)$

Prove this.