6. POWER CONGRUENCES

§6.1. Order Modulo *m*

Fermat showed that if a is not divisible by the prime p then $a^{p-1} \equiv 1 (\text{mod } p)$. This is simply an application of Lagrange's Theorem because the group $\mathbb{Z}_p^{\#}$ has order $p - 1$. Using the same argument we can extend this to an arbitrary modulus.

Theorem 1: If GCD(a, m) = 1 then $a^{\varphi(m)} \equiv 1 (\text{mod } m)$, where φ is the Euler φ-function.
Proof: Regarding a as an element of $\mathbb{Z}_m$, the fact that it is coprime to m means that it is a unit and hence is an element of $\mathbb{Z}_m^{\#}$. Since this group has order $\varphi(m)$ the result follows.

The **order of *a* modulo *m*** is the smallest positive integer n such that $a^n \equiv 1 (\text{mod } m)$. This is often called the **exponent to which *a* belongs modulo *m***, but we'll use the word "order" to remind ourselves of the group theory that lies behind it. We'll denote it by $|a|_m$.

Theorem 2: For all a that are coprime to m, $|a|_m$ divides $\varphi(m)$.

Proof: This is simply a consequence of Lagrange's Theorem that states that the order of every element of a finite group divides the order of the group.

Example 1: The orders of the numbers modulo 40 are as follows.

$\boldsymbol{a}$	1	3	7	9	11	13	17	19
$\lvert\boldsymbol{a}\rvert_{40}$	1	4	4	2	2	4	4	2

$\boldsymbol{a}$	21	23	27	29	31	33	37	39
$\lvert\boldsymbol{a}\rvert_{40}$	2	4	4	2	2	4	4	2

You'll notice that in this example, although $\varphi(40) = 16$, all of the orders are less than 16. This is simply because $\mathbb{Z}_{40}^{\#}$ isn't cyclic. In fact, $\mathbb{Z}_{40}^{\#} \cong \mathbb{Z}_8^{\#} \times \mathbb{Z}_5^{\#} \cong C_2 \times C_2 \times C_4$. Clearly the largest order of any element of this Abelian group is 4. Moreover we can use our knowledge of Abelian groups to predict that there are $2^3 = 8$ elements x where $x^2 = 1$ and so 7 elements of order 2. Also there are 16 solutions to $x^4 = 1$ in this group and hence $16 - 8 = 8$ elements of order 4. In the terminology of number theory this means that there are 7 elements where $|a|_{40} = 2$ and 8 where $|a|_{40} = 4$.

We define the **exponent** of a number m to be $e(m)$, the exponent of the group $\mathbb{Z}_m^{\#}$, that is, the smallest

positive integer n such that $a^n = 1$ in $\mathbb{Z}_m^{\#}$ for all $a \in \mathbb{Z}_m^{\#}$. Clearly $e(m)$ is the least common multiple of $|a|_m$ for $a \in \mathbb{Z}_m^{\#}$ and clearly $e(m)$ divides $\varphi(m)$.

Example 2: The following table gives $e(n)$ and $\varphi(n)$ for n up to 20.

n	1	2	3	4	5	6	7	8	9	10
$e(n)$	1	1	2	2	4	2	6	2	6	5
$\varphi(n)$	1	1	2	2	4	2	6	4	6	5

n	11	12	13	14	15	16	17	18	19	20
$e(n)$	10	2	12	6	2	4	16	6	18	4
$\varphi(n)$	10	4	12	6	8	8	16	6	18	8

Theorem 3: (1) If m, n are coprime then $e(mn) = \mathrm{LCM}(e(m), e(n))$.
(2) If p is an odd prime then $e(p^n) = \varphi(p^n) = p^{n-1}(p-1)$.
(3) If $n \geq 3$ then $e(2^n) = 2^{n-2} = \frac{1}{2}\varphi(n)$.
(4) $e(2) = e(4) = 2$.
Proof: The theorem follows from calculating the exponent of the corresponding multiplicative groups.
(1) $\mathbb{Z}_{mn}^{\#} \cong \mathbb{Z}_m^{\#} \times \mathbb{Z}_n^{\#}$.
(2) $\mathbb{Z}_{p^n}^{\#} \cong C_{p^{n-1}} \times C_{p-1}$. Since p^{n-1} is coprime to $p-1$, this is in fact cyclic.
(3) If $n \geq 3$ then $\mathbb{Z}_{2^n}^{\#} \cong C_{2^{n-2}} \times C_2$ which has exponent 2^{n-2}.

(4) is obvious.

§6.2. *p*-Order and *p*-Inertia

If p is prime and is coprime with m, the ***p*-order** of m is $|p|_m$. We'll use the alternative notation **u(*p*, *m*)**. If p, q are distinct primes the ***p*-inertia** of q is the largest y such that $p^{u(p,q)} \equiv 1 (\text{mod } q^y)$. It will be denoted by **v(*p*, *q*)**.

Example 3:
u(2, 17) = 8 because 2^n is not congruent to 1 mod 17 for $0 < n < 8$ and $2^8 \equiv 1 (\text{mod } 17)$.
v(2, 17) = 1 because 2^8 is not congruent to 1 mod 17^2.
u(2, 1093) = 364 because 2^n is not congruent to 1 mod 17 for $0 < n < 264$ and

$2^{364} \equiv 1 (\text{mod } 1093)$.
v(2, 1093) = 2 because $2^{364} \equiv 1 (\text{mod } 1093^2)$ but not mod 1093^3.
u(3, 11) = 5 because 3^n is not congruent to 1 mod 11 for $0 < n < 5$ and $3^5 \equiv 1 (\text{mod } 11)$.
v(3, 11) = 2 because 3^5 is congruent to 1 mod 11^2 but not mod 11^3.

Theorem 4: If q is prime and $t \geq 1$ and $s \geq 0$ then $(1 + kq^t)^{q^s} \equiv 1 + kq^{t+s} (\text{mod } q^{t+s+1})$, unless

$t = 1$ and $q = 2$.

Proof: $(1 + kq^t)^q \equiv 1 + kq^{t+1} + \frac{q-1}{2} k^2 q^{2t+1} + \frac{(q-1)(q-2)}{3!} k^3 q^{3t+1} + \ldots + k^q q^{tq}$

$$\equiv 1 + kq^{t+1} (\text{mod } q^{t+2})$$

except for the case $t = 1$, $q = 2$ when the last term need not be divisible by $q^3 = 8$.
Hence $(1 + kq^t)^q = 1 + k_1 q^{t+1}$ where $k_1 \equiv k (\text{mod } q)$.
By induction $(1 + kq^t)^{q^s} \equiv 1 + kq^{t+s} (\text{mod } q^{t+s+1})$.

Theorem 5: If $u = \text{u}(p, q)$ and $v = \text{v}(p, q)$ and $p^{rq^s} \equiv 1 (\text{mod } q^{s+u+1})$ for some $s \geq 1$ then $q = 2$ and $v = 1$.
Proof: We have $p^r = 1 + kq^s$ for some k where GCD$(q, k) = 1$.
Then $p^{rq^s} = (1 + kq^v)^{q^s} \equiv 1 + kq^{v+s} (\text{mod } \text{q}^{\text{v}+s+1})$ by Theorem 1 unless $q = 2$ and $v = 1$.
But $1 + kq^{v+s}$ is not congruent to 1 mod q^{v+s+1} since GCD$(q, k) = 1$.
Hence $q = 2$ and $v = 1$.

Theorem 6 (COOPER): If $2 < p < q$ are primes then $\text{u}(p, q^t) = \begin{cases} \text{u}(p, q) \text{ if } 0 < t \leq \text{v}(p, q) \\ \text{u}(p, q)\, q^{t - \text{v}(p,q)} \text{ if } t > \text{v}(p, q) \end{cases}$.
Proof: Let $u = \text{u}(p, q)$, $v = \text{v}(p, q)$ and $R = \text{u}(p, q^t)$.
If $0 < t \leq v$ then clearly $R = u$.

Suppose that $t > v$.
Since $p^u = kq^v + 1$ we have, by Theorem 4, that
$p^{uq^{t-v-1}} \equiv 1 + kq^{t-1} (\text{mod } q^t)$ for some k and
$p^{uq^{t-v}} \equiv 1 + kq^t (\text{mod } q^{t+1})$.
Thus $p^{uq^{t-v}} \equiv 1 (\text{mod } q^t)$ and so R divides uq^{t-v}.
As $p^R \equiv 1 (\text{mod } q)$, u divides R and since $p^{q-1} \equiv 1 (\text{mod } q)$, u divides $q - 1$ and so
GCD(q, u) = 1.
Thus $R = uq^{t-v-d}$ for some $d \geq 0$.
Since $p^{uq^{t-v-1}}$ is not congruent to 1 mod q^t it follows that $d = 0$.

Theorem 7: Suppose that p is an odd prime such that v(p, 2) = 1. Let $p + 1 = 2^s h$ where h is odd and suppose that v(p, 2) = 1. Then $s \geq 2$ and $u(p, 2^t) = \begin{cases} 1 \text{ if } t = 1 \\ 2 \text{ if } 2 \leq t \leq s + 1 \\ 2^{t-s} \text{ if } t > s+ 1 \end{cases}$.

Proof: If $s = 1$ then $p = 2w - 1 = 2(w - 1) + 1 = 2^2\left(\frac{w-1}{2}\right) + 1$ where $\frac{w-1}{2}$ is an integer.
Consequently $p \equiv 1 (\text{mod } 2^2)$ contrary to the fact that v(p, 2) = 1.
(1) Obviously u(p, 2) = 1.

(2) $p^2 = (2^s w - 1)^2 = 2^{2s} w^2 - 2^{s+1} w + 1 \equiv 1 (\text{mod } 2^{s+1})$ which proves the theorem for
$2 \le t \le s + 1$.
(3) By (2) $p^2 = 1 + k2^{s+1}$ for some k with $0 < k < 2^{s+1}$.
Applying Theorem 4, if $t \ge s + 1$,
$(p^2)^{2^{t-s-1}} = (1 + k2^{s+1})^{2^{t-s-1}}$ and so $p^{2^{t-s}} \equiv 1 + k2^t (\text{mod } 2^{t+1})$.
Similarly $p^{2^{t-s-1}} \equiv 1 + k2^{t-1} (\text{mod } 2^t)$.
Thus $p^{2^{t-s}} \equiv 1 (\text{mod } 2^t)$. But $p^{2^{t-s-1}}$ is not congruent to 1 mod 2^t.
Clearly $u(p, 2^t)$ divides 2^{t-s} and hence must be a power of 2 greater than 2^{t-s-1}.
Consequently $u(p, 2^t) = 2^{t-s}$.

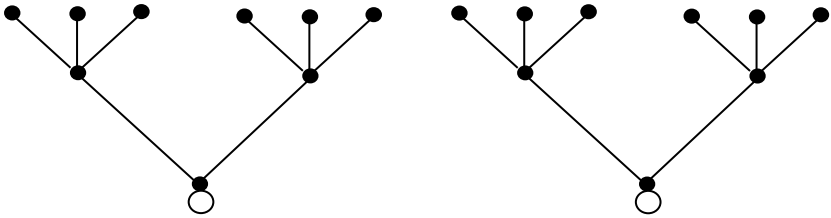
Having $v(p, 2)$ bigger than 1 is not very common. The smallest prime p for which this is the case is $p = 1093$, for which $u(p, 1) = 364$.

§6.3. Application to Group Theory

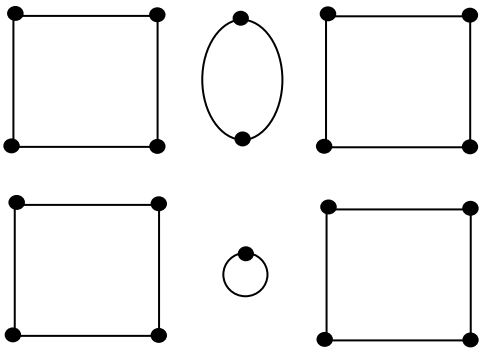
Suppose that G, H are two finite groups. A ***p*-isomorphism** is a 1-1 and onto map
f:G $\rightarrow$ H such that $f(x^p) = f(x)^p$. We say that G, H are ***p*-isomorphic** if there exists a p-isomorphism between them and we write G $\cong_p$ H. This is a weaker condition than isomorphism.

We can illustrate *p*-isomorphism graphically. Define the ***p*-graph** of a finite group G by taking the elements of G as vertices and drawing an undirected edge between *g* and *h* if one of these elements is the *p*'th power of the other. Clearly if $g \in G$ has order p^n then it's part of a tree in the *p*-graph (with a small loop at 1). If *g* has order *m*, coprime to *p*, then *g* lies in a cycle of length u(*p*, *m*).

Example 4: The 3-graph of C_{18} is



Example 5: The 3-graph of C_{20} is



Clearly two groups are *p*-isomorphic if and only they have the same *p*-graph. A closely related concept is that of conformality. A **conformality** from G to H is a 1-1 and onto map f:G→H that preserves the orders of the elements, that is, if $|f(g)| = |g|$ for all $g \in G$. Groups G, H are **conformal** if there exists a conformality between them and we write **G ≈ H**. If G, H are finite then G ≈ H if and only if these groups have the same number of elements of each order.

Example 6: Let $G = C_{11} \times C_{11} \times C_{121}$ and $H = C_{121} \times C_{121}$. Show that $G \cong_3 H$ but $G \not\approx H$.
Solution: The smallest n such that $3^n \equiv 1 (\text{mod } 11)$ is $n = 5$. Since $v(3, 11) = 2$, the smallest n such that $3^n \equiv 1 (\text{mod } 121)$ is also 5. Therefore the 3-graphs of G and H both consist of 1 cycle of length 1 and $\frac{11^4 - 1}{5} = 2928$ cycles of length 5. They are therefore 3-isomorphic. However G has $11^3 - 1 = 1330$ elements of order 11 while H has only 120 elements of order 11. Hence G, H are not conformal.

It's clear that if p is prime and G, H are p-groups then $G \cong_p H$ implies that $G \approx H$. This conclusion holds, in certain cases, when G, H are q-groups for some prime $q \neq p$.

Theorem 8 (COOPER): Suppose $2 < q < p$ are primes where $v(p, q) = 1$. If G, H are q-groups then $G \sim_p H$ implies that $G \approx H$.

Proof: Let f:G→H be a p-isomorphism. Suppose that $g \in G$ has order q^r and suppose that $f(g)$ has order q^s. The length of the cycle containing g in the p-graph of G is $u(p, q^r)$ and the length of the cycle containing $f(g)$ is $u(p, q^s)$. Hence $u(p, q^r) = u(p, q^s)$. By Theorem 6, $u(p, q)q^{r-1} = u(p, q)q^{s-1}$ and so $r = s$. Hence f is a conformality.