The Structure of G_n

<u>Notation</u> If $a \in G_n$ we write $|a|_n$ for the order of a.

e.g. $|4|_5 = 2$ $|2|_5 = 4$

A finite group G is <u>cyclic</u> if there is an element $a \in G$ such that $G = \{a^i : 1 \le i \le n\}$

This means that the <u>order</u> of a is $|G|$ – no. of elements of G.

<u>Examples</u> G_3 is cyclic since $G_3 = \{2, 2^2\}$

$G_5 = \{2, \underset{4}{2^2}, \underset{3}{2^3}, \underset{1}{2^4}\}$ is cyclic

$G_9 = \{1, 2, 4, 5, 7, 8\}$ is cyclic since

$G_9 = \{1, 2, 2^2, \underset{8}{2^3}, \underset{7}{2^4}, \underset{5}{2^5}\}$

G_7 is cyclic since $G_7 = \{\underset{3^6}{1}, 3, \underset{2}{3^2}, \underset{6}{3^3}, \underset{4}{3^4}, \underset{5}{3^5}, \cancel{3^6}\}$

<u>Defn</u> a is a <u>primitive element</u> of G_n (or mod n)

if $G_n = \{a^i : 1 \le i \le \phi(n)\}$, equivalently if

$|a|_n = \phi(n) = |G_n|$ <u>Related</u> to primitive roots of unity

Primitive element

~~52~~ (54)

Theorem If p is prime then G_p contains a primitive element. Hence G_p is cyclic.

Proof later.

Structure theorem for finite abelian groups

If H is a finite abelian group then

$$H \cong H_1 \times \cdots \times H_r \quad \text{for some } r \text{ where}$$

each H_i is cyclic.

(the decomposition can also be chosen so that $|H_i| = p_i^{k_i}$ for p_i prime and $k_i \geq 1$. $p_i = p_j$ is possible)

Examples G_n is cyclic for $n = 2, 3, 5, 7, 9, 4, 6$

G_2 is trivial. G_3, G_4 and G_6 are cyclic of order 2

G_7, G_9 cyclic of order 6

G_5 is cyclic of order 4.

G_8 is ~~the produ~~ isomorphic to the product of 2 cyclic groups of order 2. This is often written

$$G_8 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \text{ where } \mathbb{Z}_2 \text{ is a commutative group}$$

under addition.

We have seen that if $n = n_1 \times \cdots \times n_r$ with $\gcd(n_i, n_j) = 1$ for $i \neq j$ then $G_n \cong G_{n_1} \times \cdots \times G_{n_r}$ ~~But is G~~

When is G_n cyclic? More generally, what is the lcm of the orders of elements of G_n?

65

Lemma If H is any group and $a \in H$ has order n then $a^m = 1 \iff n \mid m$

Proof ~~Theorem~~ Write $m = kn + r$ $0 \le r < n$ $a^m = (a^n)^k \times a^r \Rightarrow a^r = 1 \Rightarrow r = 0$ by defn of order $\square$

Lemma If $H \cong H_1 \times H_2$ ~~where~~ H_1 and H_2 are finite cyclic groups then H is cyclic $\iff$ $\gcd(|H_1|, |H_2|) = 1$

In all cases, the order of every element of H is a divisor of $\mathrm{lcm}(|H_1|, |H_2|)$

Proof Write $n_1 = |H_1|$, $n_2 = |H_2|$ and $n = \mathrm{lcm}(n_1, n_2)$

If $(a_1, a_2) \in H_1 \times H_2$ then $a_1^{n_1} = 1 \Rightarrow a_1^n = 1$ $a_2^{n_2} = 1 \Rightarrow a_2^n = 1$

So $(a_1, a_2)^n = (1,1)$ and the order of (a_1, a_2) is a divisor of n. Since $H \cong H_1 \times H_2$ the order of a is a divisor of n $\forall a \in H$

$|H_1 \times H_2| = n_1 n_2$ so if $H_1 \times H_2$ is cyclic, $\mathrm{lcm}(n_1, n_2) = n_1 n_2$ and $\gcd(n_1, n_2) = 1$

~~Conversely if $(a_1, a_2)^m = (a_1^m, a_2^m) = (1,1)$ then~~

n_1 ~~$\mid m$ and n_2~~

Now suppose that H_1 and H_2 are cyclic and $\gcd(n_1, n_2) = 1$. Then let a_1 and a_2 be generators (= primitive elements) of H_1 and H_2, that is

$H_1 = \{a_1^j : 1 \le j \le n_1\}$ $H_2 = \{a_2^j : 1 \le j \le n_2\}$

and a_1, a_2 have orders n_1, n_2 respectively.

Then (a_1, a_2) is a generator of $H_1 \times H_2$. To see this:

it suffices to show (a_1, a_2) has order $n_1 n_2$

So suppose $(a_1, a_2)^n = (a_1^n, a_2^n) = 1$ then $n_1 \mid n$ and $n_2 \mid n$

So $n_1 n_2 \mid n$ and since $n \mid n_1 n_2$, $n = n_1 n_2$ $\square$

~~54~~ 56

If n is composite then G_n is often not cyclic. The reason is:

Lemma If $n \in \mathbb{Z}_+$, $n > 2$ then $\phi(n)$ is even.

Proof If p is an odd prime then $\phi(p) = p-1$ is even.

If n is divisible by an odd prime p then $n = n_1 \times p^k$ some $k \geqslant 1$ where $\gcd(n_1, p) = 1 = \gcd(n_1, p^k)$

$$\phi(n) = \phi(n_1) \times \phi(p^k) = \phi(n_1) \times p^{k-1}(p-1) \text{ is even.}$$

If $n > 2$ and n is not divisible by any odd prime then $n = 2^k$ $k \geqslant 2$ $\phi(n) = 2^{k-1}$ is even.

Corollary If $n = n_1 n_2$ where $\gcd(n_1, n_2) = 1$ and $n_1, n_2 > 2$ then G_n is not cyclic

Proof $\phi(n_1)$ and $\phi(n_2)$ are even and $\phi(n) = \phi(n_1)\phi(n_2)$

So $2 \mid \gcd(\phi(n_1), \phi(n_2))$

So $G_n \cong G_{n_1} \times G_{n_2}$ is not cyclic.

Examples G_{12} is not cyclic, G_{15} not cyclic,
$G_{12} \cong G_3 \times G_4 = \{1,2\} \times \{1,3\}$ has 4 elements but every element has order 1 or 2 $\quad G_{15} \cong G_3 \times G_5 = \{1,2\} \times \{1,2,3,4\}$ has 8 elements but every element has order 1, 2 or 4

Another result we need for the Primitive Element Theorem is the

We have also seen that if $n = n_1 \times n_2$, $\gcd(n_1, n_2) = 1$ then $a^{\ell} \equiv 1 \mod n$ $\forall a \in G_n$ $\left(\ell = \operatorname{lcm}(\phi(n_1), \phi(n_2))\right)$
e.g. this happens with $n_1 > 2$ & $n_2 > 2$ then $\ell \mid \frac{\phi(n)}{2} = \frac{\phi(n_1)\phi(n_2)}{2}$ $\quad$ Example $n = 56$ $\phi(7) = 6$ $\phi(8) = 2$ $\operatorname{lcm}(\phi(7)\phi(8)) = 6$ $\quad n = 91 = 7 \times 13$ $\phi(7) = 6$ $\phi(13) = 12$

Fundamental Lemma

If $N \in \mathbb{Z}_+$,

$$N = \sum_{d \mid N} \phi(d)$$

Check $N = 20$ $\phi(5) = 4$ $\phi(1) = 1$ $\phi(4) = 2$ $\phi(10) = 4$ $\phi(20) = \#\{1,3,7,11,13,17,19,9\} = 8$

Proof $\{k : 1 \leq k \leq N\}$ is the disjoint union of sets $\{k : 1 \leq k \leq N, \gcd(k, N) = d\}$

<u>Examples</u> $12 = 4 \times 3$ $\quad G_{12} \cong G_3 \times G_4$ is not cyclic.

Every element is of order 1 or 2 (4 elements)

$15 = 5 \times 3$ $\quad G_{15} \cong G_5 \times G_3$ is not cyclic.

We have also seen that if $n = n_1 \times n_2$ and $\gcd(n_1, n_2) = 1$

then $a^l \equiv 1 \mod n$ $\forall a \in G_n$, where $l = \operatorname{lcm}(\phi(n_1), \phi(n_2))$

This is because $G_n \cong G_{n_1} \times G_{n_2}$ and $\phi(n_i) = |G_{n_i}|$

<u>Examples</u> $n = 56$. $\phi(56) = \phi(8) \times \phi(7) = 4 \times 6 = 24$

but $\operatorname{lcm}(4, 6) = 12$.

So $a^{12} \equiv 1 \mod 56$ $\quad \forall a \in G_{56}$

This is better than Euler's Theorem. but we can do even better.

Every element of G_8 has order 1 or 2. $\operatorname{lcm}(2, 6) = 6$

So $a^6 \equiv 1 \mod 56$ $\quad \forall a \in G_{56}$.

This is the best possible. (because G_7 is cyclic)

<u>Example</u> $n = 91$. $\phi(91) = \phi(13) \times \phi(7) = 12 \times 6 = 72$

$\operatorname{lcm}(12, 6) = 12$ $\quad a^{12} \equiv 1 \mod 91$ $\forall a \in G_{91}$

This is the best possible (G_{13} is cyclic)

<u>Example</u> Can 110 be $\phi(N)$. 111 not prime.

But $\phi(p^k) = p^{k-1}(p-1)$ if p prime and $110 = 11(11-1)$

So $\phi(11^2) = 110$ $\quad 11^2 = 121$ $\quad a^{110} \equiv 1 \mod 121$ $\forall a$ coprime to 11.

<u>Always</u> if $n_1 > 2$ and $n_2 > 2$ and $\gcd(n_1, n_2) = 1$ then

$\phi(n_1) \mid \phi(n_1) \cdot \frac{\phi(n_2)}{2}$ $\qquad \phi(n_2) \mid \frac{\phi(n_1)}{2} \cdot \phi(n_2) = \frac{\phi(n)}{2}$

So $a^{\frac{\phi(n)}{2}} \equiv 1 \mod n$ $\quad \forall a \in G_n$.

Again, this is better than Euler's Theorem.

<u>Fundamental Lemma</u> If $N \in \mathbb{Z}_+$, $N = \sum_{d \in \mathbb{Z}_+,\, d \mid N} \phi(d)$

<u>Check</u> $N = 20 = 2^2 \times 5$. Divisors are $1, 2, 4, 5, 10, 20$.
$\phi(1) = 1 = \phi(2)$ $\phi(4) = 2$ $\phi(5) = \phi(5 \times 2) = 4$ $\phi(20) = \phi(4) \times \phi(5) = 8$

$1 + 1 + 2 + 4 + 4 + 8 = 20$

<u>Check</u> $N = 110 = 2 \times 5 \times 11$ Divisors are $1, 2, 5, 11, 10, 22, 55, 110$
$\phi(1) = 1 = \phi(2)$ $\phi(5) = 4 = \phi(5 \times 2) = \phi(10)$ $\phi(11) = 10 = \phi(22)$ $\phi(55) = \phi(5) \times \phi(11) = 40$
$\phi(110) = \phi(5) \times \phi(11) \times \phi(2) = 4 \times 10 = 40$ $1 + 1 + 4 + 4 + 10 + 10 + 40 + 40 = 110$

<u>Proof of Lemma</u> d is a divisor of $N \Leftrightarrow \frac{N}{d}$ is a divisor of N $\frac{N}{(N/d)} = d$
$\{k : 1 \le k \le N, k \in \mathbb{Z}_+\}$ is the disjoint union of sets $A_d = \{k \in \mathbb{Z}_+ : \gcd(k, N) = d,\ 1 \le k \le N\}$ where d is a divisor of N

$A_d = \{k_1 d : k_1 \in \mathbb{Z}_+, 1 \le k_1 \le \frac{N}{d}, \gcd(k_1, \frac{N}{d}) = 1\}$ if $d \mid N$

So $\#(A_d) = \phi(\frac{N}{d})$. So $N = \sum_{d \in \mathbb{Z}_+, d \mid N} \#(A_d) = \sum_{d \in \mathbb{Z}_+, d \mid N} \phi(\frac{N}{d}) = \sum_{\substack{d' \in \mathbb{Z}_+ \\ d' \mid N}} \phi(d')$ $\square$

<u>The ring $\mathbb{Z}_p[x]$</u>

The proof of the Primitive Element Theorem uses the fact that, if $p \in \mathbb{Z}_+$ is prime, then the ring $\mathbb{Z}_p[x] = \{a_0 + a_1 x + \dots + a_n x^n : n \in \mathbb{N}, a_i \in \mathbb{Z}_p, 0 \le i \le n\}$ is a <u>unique factorisation domain</u> (UFD)

This means that $\mathbb{Z}_p[x]$ is:

- is a commutative ring with identity
- has no zero divisors.
- has unique factorisation into <u>irreducibles</u> – which are also <u>primes</u>, since this is a UFD.

The <u>units</u> in $\mathbb{Z}_p[x]$ are the constant polynomials $a_0 \in \mathbb{Z}_p^*$ (so not including 0)

<u>Def^n</u> A non-constant polynomial f is <u>irreducible</u> (in $\mathbb{Z}_p[x]$) if it cannot be written in the form $f_1 f_2$ where both f_1, f_2 are not units

Examples

Any polynomial a_0+a_1x, for $a_1 \in \mathbb{Z}_p^*$, is irreducible in $\mathbb{Z}_p[x]$ - because if we write $a_0+a_1x = f_1f_2$ for polynomials f_1 and f_2, one of f_1 and f_2 must be a non zero constant.

But there are many other examples.

Consider x^2+x+1 in $\mathbb{Z}_p[x]$ for various p.

If $x^2+x+1 = f_1f_2$ where neither f_1 nor f_2 is constant, we must have $f_1 = b_1x+b_0$ $f_2 = c_1x+c_0$, for $b_1, c_1 \in \mathbb{Z}_p^*$, $b_1c_1 = 1$. Then $f_1f_2 = (x+b_0b_1^{-1})(x+c_0c_1^{-1})$
$= (x-\beta)(x-\gamma)$ $\quad \beta = -b_0b_1^{-1}$ $\quad \gamma = -c_0c_1^{-1}$

e.g. in $\mathbb{Z}_3[x]$ $\quad x^2+x+1 = (x+2)(x+2) = (x-1)(x-1)$. So x^2+x+1 is reducible because $x^2+x+1 = x^2-2x+1$. But x^2+x+1 is irreducible in $\mathbb{Z}_2[x]$ and in $\mathbb{Z}_3[x]$.. $\mathbb{Z}_5[x]$ (for example)

Fact $x-a \mid f(x)$ in $\mathbb{Z}_p[x]$ (for p prime) $\Leftrightarrow f(a)=0$

This is because we can find $g(x) \in \mathbb{Z}_p[x]$ and $b \in \mathbb{Z}_p$ s.t.
$f(x) = g(x)(x-a) + b$ $\quad f(a) = b$ $\quad$ so $f(a)=0 \Leftrightarrow f(x) = g(x)(x-a)$ for some $g \in \mathbb{Z}_p[x]$. In $\mathbb{Z}_2[x]$: $0^2+0+1 = 1 = 1^2+1+1 \neq 0$

In $\mathbb{Z}_5[x]$ $\quad a^2+a+1 \neq 0$ for any of $a = 0, 1, 3, 3, 4$.

<u>Unique factorisation</u> means that if $f \neq 0$ and $f \neq$ unit then

$$f = \alpha \prod_{j=1}^{s} f_j^{k_j}$$ where α is a unit, $k_j \in \mathbb{Z}_+$, f_j irreducible and $f_i \neq$ unit $\times f_j$ for $i \neq j$. Moreover this expression is <u>unique</u> in the following sense

If $f = \alpha \prod_{j=1}^{s} f_j^{k_j} = \beta \prod_{j=1}^{t} g_j^{m_j}$ are two expressions of this type, then $s = t$ and after reordering, $k_j = m_j$ and $g_j = \alpha_j f_j$ for some unit α_j $\forall\, 1 \le j \le s$.

The Primitive Element Theorem can be strengthened to:

<u>Theorem</u> Let p be prime. Then for each divisor d of $p-1$, there are $\phi(d)$ elements of order d in G_p $(= \mathbb{Z}_p^*)$. In particular, there are $\phi(p-1)$ <u>primitive</u> elements in G_p.

<u>Remarks</u> 1. $p-1 = \sum_{d \mid p-1} \phi(d)$ by the Fundamental Lemma.

2. $\phi(d) > 0$ $\forall d \in \mathbb{Z}_+$ because $\phi(1) = 1$ and if $d > 1$ and q is a prime divisor of d then $\phi(q) \mid \phi(d)$ and $\phi(q) = q-1$. So $\neq 0$

<u>Proof of Theorem</u> $a^{p-1} \equiv 1 \bmod p$ $\forall a \in G_p$ by Fermat's Little Theorem.

So $x - a \mid x^{p-1} - 1$ $\forall a \in \mathbb{Z}_p^*$.

So, since $\mathbb{Z}_p[x]$ is a UFD, $x^{p-1} - 1 = \prod_{a \in \mathbb{Z}_p^*} (x - a)$ coeffs of x^{p-1} agree.

We want to show that $\exists a \in \mathbb{Z}_p^*$, $a^d \neq 1$ for any proper divisor d of $p-1$. For each such d, $x^d - 1 \mid x^{p-1} - 1$, because, if $p-1 = dk$

$$x^{p-1} - 1 = (x^d - 1) \sum_{j=0}^{k-1} x^{jd}$$

So $x^d - 1$ is a product of d <u>distinct</u> linear factors $x - a_{j,d}$ $1 \le j \le d$

So $a^d \equiv 1 \bmod p \iff a = a_{j,d}$, some j.

So for each divisor d of $p-1$ there are exactly d elements of order dividing d. We claim that there are $\phi(d)$ elements of order d.

We prove this by induction on d. Clearly true for $d = 1$. Assume true for $1 \le d_1 < d$. In particular it is true for $d_1 \mid d$, $1 \le d_1 < d$.

But $d = \phi(d) + \sum_{1 \le d_1 < d,\, d_1 \mid d} \phi(d_1)$. So there are $\phi(d)$ elements of order exactly d, as required $\square$

How do we find primitive elements?

Recall $|a|_p$ is the order of a mod p.

<u>Lemma</u> If $k \in \mathbb{Z}_+$, $\quad |a^k|_p = \dfrac{|a|_p}{\gcd(k, |a|_p)}$

In particular if a is primitive then a^k is primitive $\iff \gcd(k, |a|_p) = 1 \iff \gcd(k, p-1) = 1$

<u>Proof</u> $a^{km} = 1 \iff |a|_p \mid km$ $\quad$ Write $k = k_1 k_2$ where

$k_1 = \gcd(k, |a|_p)$ $\quad$ Then $\gcd\left(k_2, \dfrac{|a|_p}{k_1}\right) = 1$

$$|a|_p \mid km \iff \frac{|a|_p}{k_1} \mid k_2 \times m \iff \frac{|a|_p}{k_1} \mid m.$$

So $|a^k|_p = \dfrac{|a|_p}{k_1}$ $\quad \square$

<u>Example</u> Find ~~all elements of all~~ the primitive elements of G_{31}. Also find ~~the orders of all elements of G_{31}~~ an element of G_{31} of each possible order.

$30 = 31 - 1$ - divisible by $2, 3, 5, 6, 10, 15, 30$

2 is not primitive because $2^5 \equiv 1 \mod 31$.

Since 5 is prime, 2 has order 5. $\quad 2^j$ also has order 5 for $j = 2, 3, 4$

$3^2 \equiv 9 \quad 3^3 \equiv 27 \equiv -4 \quad \cancel{3^4 = 81 \equiv 19} \quad 3^5 \equiv 9 \times -4 \equiv -5$

$3^6 \equiv (-4) \times (-4) \equiv 16 \qquad 3^{10} \equiv 25 \qquad 3^{15} \equiv -125 \equiv -1$

So 3 is primitive. $\qquad \phi(30) = \phi(2) \times \phi(3) \times \phi(5) = 8$

The other primitive elements are 3^j for $j = 7, 11, 13, 17, 19, 23, 29$

$3^7 \equiv 16 \times 3 \equiv 17$

$3^{11} \equiv 16 \times -5 \equiv -80 \equiv +13 \equiv 18$

$3^{13} \equiv -18 \times 9 \equiv -162 \equiv -7$

$3^{17} \equiv -7 \times 9 \times 9 \equiv 1 \times 9 \equiv 9 \equiv 22$

$3^{19} \equiv -9 \times 9 \equiv -81 \equiv -19$

$3^{23} \equiv 19 \times 9 \times 9 \equiv 171 \times 9 \equiv 16 \times 9 \equiv 144 \equiv 20 \equiv +11$

$3^{29} \equiv 16 \times 20 \equiv 320 \equiv 10 \equiv -10 = 21$

So altogether the primitive elements are $3, \underset{24}{-7}, 9, \underset{21}{-10}, 17, \underset{13}{-18}, \underset{12}{-19}, -20 = 11$

$3, \cancel{9}, 11, 12, 13, 17, 21, 24, 22$

Elements of order 2, 3, 5, 6, 10, 15 are

$-1, \ -6 (\equiv 3^{10}), \ 2, \ -5 (\equiv 3^{6}), \ -4 (\equiv 3^{3}) \ \ 9 (\equiv 3^{2})$

resp.

-1 is the only element of order 2, there are 2 elements of order 3, 4 of order 5, 2 of order 6, $4 = \phi(10)$ of order 10 and $8 = \phi(15)$ of order 15.

<u>How to find an element of order ~~all~~</u> $\mathrm{lcm}(n_1, n_2)$

Suppose we have an element a_1 of order n_1 and ~~and~~ element a_2 of order n_2. How can we find an element of order n where $n = \mathrm{lcm}(n_1, n_2)$?

What about $a_1 a_2$? <u>Yes</u> if $\gcd(n_1, n_2) = 1$ – not otherwise in general.

Suppose $(a_1 a_2)^k = 1$

Then $a_1^k = a_2^{-k}$

The order of a_1^k is $\dfrac{n_1}{\gcd(k, n_1)}$ and the order of a_2^{-k} is $\dfrac{n_2}{\gcd(k, n_2)}$

~~So both these are divisors of k n_1~~ divisors of n_1 & n_2 resp.

$1 = \gcd(n_1, n_2) \Rightarrow \text{order}(a_1^k) = \text{order}(a_2^k) = 1$

i.e. $a_1^k = 1 = a_2^{-k}$

So $n_1 \mid k$ and $n_2 \mid k$ So $n_1 n_2 \mid k$ and $a_1 a_2$ has order $n_1 n_2$.

~~If $\gcd(n_1, n_2) > 1$ then we can find n_2' such that~~

~~84~~ 63

The structure of G_{p^k}

We have seen that if $n = \prod_{i=1}^{r} p_i^{k_i}$ for distinct primes p_i

then $G_n \cong G_{p_1^{k_1}} \times \cdots \times G_{p_r^{k_r}}$

G_p is cyclic if p is prime. But what about G_{p^k} for $k \geq 2$?

It cannot always be cyclic because $G_{2^3} = G_8$ is not cyclic

$G_8 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. However, the following theorem is due to Gauss:

Theorem For all $k \geq 2$

$G_{2^k} \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$ $\quad G_4 \cong \mathbb{Z}_2$, $G_8 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, $G_{16} \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \cdots$

If p is prime ≥ 3 then G_{p^k} is cyclic (of order $p^{k-1}(p-1)$)

Remark $\mathbb{Z}_1$ is the trivial group (with just one element - the identity element - called 0 since we call the group operation $+$)

Proof of Theorem We will show that in G_{2^k}, $2^{k-1}+1$ has order $2 \bmod 2^k$

$1+2$ has order $2^{k-2} \bmod 2^k$ $\forall k \geq 3$

and ~~if p is prime ≥ 3 then~~

If p is prime ≥ 3 then $1+p$ has order $p^{k-1} \bmod p^k$

This shows that G_{2^k} has 2 elements of order 2 if $k \geq 3$ because

$-1 \equiv 2^k - 1 \not\equiv 2^{k-1}+1$ has order 2. So G_{2^k} is not cyclic for $k \geq 3$

because if it were there would be only $\phi(2) = 1$ element of order 2.

But since $1+2$ has order 2^{k-2} it contains a cyclic group of order 2^{k-2}

and must be isomorphic to $\mathbb{Z}_{2^{k-2}} \times \mathbb{Z}_2$ since it has 2^{k-1} elements.

~~On the But If p is prime ≥ 3 then G_{p^k} contains an element of order p^{k-1}~~

~~But A also contains an element a such that a~~

But if p is prime $p \geqslant 3$ then G_{p^k} also contains a such that $a^{p-1} \equiv 1 \bmod p$

$a^k \not\equiv 1 \bmod p \quad 0 < k < p-1.$

Then the order of $a \bmod p^k$ must be a multiple of $p-1$.

$\gcd(p-1, p^{k-1}) = 1$. So G_{p^k} must contain an element of order $p^{k-1}(p-1)$: Some a^n has order $p-1$, $1+p$ has order p^{k-1}

$a^n(1+p)$ has order $p^{k-1}(p-1)$ and is primitive

Lemma $p \mid \binom{p}{k} \ \forall\ 1 \leq k \leq p-1$. This was on Problem Sheet 3.

Lemma 3 has order $2^{k-2} \bmod 2^k \ \forall k \geqslant 3$

If p is prime $\geqslant 3$ then $1+p$ has order $p^{k-1} \bmod p^k$.

Proof. By induction

$$(1+2)^{2^m} = 1 + 2^{m+2} + C_m 2^{m+3} \quad \forall m \geqslant 1$$

$$(1+2)^2 = 1 + 2^3$$

If true for $m \geqslant 1$ $(1+2)^{2^{m+1}} = \left(1+2^{m+2}+C_m 2^{m+3}\right)^2 = 1+2^{m+3} + 2C_m 2^{m+4} + O(2^{2m+4})$

By induction for p prime $\geqslant 3$

$$(1+p)^{p^m} = 1 + p^{m+1} + C_m p^{m+2}$$

$m=1$ $$(1+p)^p = \sum_{k=0}^{p} \binom{p}{k} p^k$$ $\binom{p}{1}$ and $\binom{p}{2}$ both divisible by p.

<u>Lemma</u> If p is prime and $\gcd(a,p)=1$ then $\forall k \in \mathbb{Z}_+$

$|a|_{p^{k+1}} = |a|_{p^k}$ or $p.|a|_{p^k}$.

<u>Proof</u> If $a^n \equiv 1 \mod p^{k+1}$ then $a^n \equiv 1 \mod p^k$

So $|a|_{p^k} \mid |a|_{p^{k+1}}$

Put $m = |a|_{p^k}$

$a^m = 1 + bp^k$

If $p \mid b$ then $|a|_{p^{k+1}} = |a|_{p^k}$

Otherwise $\gcd(b,p)=1$

$a^{rm} = 1 + brp^k + O(p^{2k}) \quad (= (1+bp^k)^r$

$a^{rm} \equiv 1 \mod p^{k+1} \iff br \equiv 0 \mod p$

$\iff r \equiv 0 \mod p$

So if $|a|_{p^{k+1}} \neq |a|_{p^k}$ we have $|a|_{p^{k+1}} = p.|a|_{p^k}$.

Miller Rabin Test

The Miller Rabin Primality test is based on the following lemma.

<u>Lemma</u> Suppose n is an odd prime and $1 < a < n$.
Write $n-1 = 2^s d$ for odd d and $s \geq 1$.
Then either $a^d \equiv 1 \mod n$ or for some r with $0 \leq r \leq s$
we have $a^{2^r \cdot d} \equiv -1 \mod n$.

<u>Proof</u> If n is prime then by Fermat's Little Theorem

$a^{n-1} \equiv 1 \mod n$. $\forall\ 1 \leq a < n$.

That is $a^{2^s d} \equiv 1 \mod n$. Suppose $a > 1$.

Then either $a^d \equiv 1 \mod n$ or there is $r \geq 0$ such that
$a^{2^r d} \not\equiv 1 \mod n$ but $a^{2^{r+1} d} \equiv 1 \mod n$.

<u>Claim</u> $a^{2^r d} \equiv -1 \mod n$.
This is because $a^{2^r d}$ has order 2 and there
is just $1 = \phi(2)$ element of order 2 mod n.
This can be seen directly by unique factorisation
in $\mathbb{Z}_n[x]$. $x^2 - 1 = (x-1)(x+1)$
the only solutions to $x^2 \equiv 1 \mod n$ must
therefore be $x \equiv \pm 1 \mod n$.

Applications of the Structure of G_n

Here is an application to the ~~fact~~ possible orders of elements of G_q, q prime.

__Theorem__ Let ~~p and~~ q be primes. Let $n \in \mathbb{Z}_+$

Then $q \mid \dfrac{p^n - 1}{p-1} \iff$ either $p \equiv 1 \bmod q$ and $q \mid n$
or $\gcd(n, q-1) = k > 1$ and $p^k \equiv 1 \bmod q$

__Proof__ First suppose $p \equiv 1 \bmod q$, which means $q \mid p-1$.

Then $\dfrac{p^n-1}{p-1} = \sum_{k=0}^{n-1} p^k = \sum_{k=0}^{n-1} (1+(p-1))^k = n + \underbrace{a(p-1)}_{\text{divisible by } q}$ some a

This is divisible by $q \iff q \mid n$.

Now suppose $p \not\equiv 1 \bmod q$

Then $q \mid \dfrac{p^n-1}{p-1} \iff q \mid p^n - 1$ because $\gcd(q, p-1) = 1$ (uses q prime.

$p^n - 1 \equiv 0 \bmod q \iff \gcd(n, q-1) = k > 1$
with $p^k \equiv 1 \bmod q$

__Example__ When does $7 \mid \dfrac{3^n - 1}{3-1}$?

$3 \not\equiv 1 \bmod 7$. What is the order of 3 mod 7 ? 6.

So $7 \mid \dfrac{3^n-1}{3-1} \iff 7 \mid 3^n - 1 \iff 3^n \equiv 1 \bmod 7$

$\iff 6 \mid n$. Check $3^6 = 729$ $\dfrac{728}{2}$: 364 is divisible by 7.

When does $2 \mid \dfrac{3^n-1}{3-1}$? $3 \equiv 1 \bmod 2$ so $2 \mid \dfrac{3^n-1}{3-1}$

$\iff$ n is even.

67

Miller Rabin examples

$n = 49.$ $\quad a = 2 \quad 2^{48} \equiv 15$

$a = 30 \quad 30^{48} \equiv 1 \quad 30^{24} \equiv 1 \quad 30^{12} \equiv \cancel{28}\ 1$

$30^{6} \equiv 1 \quad 30^{3} \equiv 1$

$n = 91 \quad a = 2 \quad 2^{90} \equiv 64 \mod 91.$

$a = 16 \quad 16^{45} \equiv 1$ Miller Rabin fails.

$n = 221 \quad a = 174 \quad a^{220} \equiv 1 \mod 221$

$a^{110} \equiv -1 \mod 221$

However $\left(a = 137 \quad a^{220} \equiv 35 \mod 221\right)$

$a = 2 \quad a^{220} \equiv 16 \mod 221$

$a = 38 \quad 38^{220} \equiv 1 \mod 221$

$38^{110} \equiv 118 \not\equiv 1 \mod 221$ Miller Rabin works

$(118 \equiv -1 \mod 17 \quad 118 \equiv 1 \mod 17)$

$n = 1189 \quad 204^{1188} \equiv 1 \mod 1189$

$204^{594} \equiv 1 \mod 594$

$204^{297} \equiv 204 \mod 297$

Miller Rabin works (it's a coincidence that we get 204 again)

Examples using primitive roots

Find all x such that $2^x \equiv 3 \mod 11$ (if any)

$2^5 \equiv -1 \mod 11$ So 2 is primitive

$3^5 \equiv 1 \mod 11$ $(3^5 = 243)$

So $3 = 2^{2y}$ for some y.

$2^3 = 8 \equiv -3$ so $2^8 \equiv 3 \mod 11$

$$2^x \equiv 3 \mod 11 \Leftrightarrow 2^x = 2^8 \mod 11$$

$\Leftrightarrow x \equiv 8 \mod 10.$

Another example Find all x such that $5^x = 3 \mod 11$ (if any)

$3 \equiv 2^8$ $5 \equiv 2^4 \equiv 16 \mod 11$

$5^x \equiv 2^{4x} \equiv 2^8 \Leftrightarrow 2^{4(x-2)} \equiv 1 \mod 11 \Leftrightarrow 4(x-2) \equiv 0 \mod 10$

$\Leftrightarrow 4x \equiv 8 \mod 10 \Leftrightarrow 2x \equiv 4 \mod 5$

$\Leftrightarrow x \equiv 2 \mod 5$

Another example Find all y such that

$$y^5 \equiv 1 \mod 11$$

$y \equiv 1$ or 4 elements of order 5 3^n for $n = 1, 2, 3, 4$.

Carmichael numbers (79)

A *Carmichael number* is a composite number n such that every $m \in G_n$ satisfies $m^{n-1} \equiv 1 \mod n$.

The idea is that such numbers are relatively hard to prove primality of. — though we are still restricting to $m \in G_n$.

Infinitely many Carmichael numbers are known.

Korselt's Criterion $n = \prod_{j=1}^{r} p_j^{k_j}$ is a Carmichael number if and only if

$$k_j = 1 \quad \forall\ 1 \le j \le r$$

$$\text{and } p_j - 1 \mid n-1 \quad \forall\ 1 \le j \le r.$$

Idea of proof The orders of elements of $G_n \cong \prod G_{p_j^{k_j}}$ are $\operatorname{lcm}(p_j^{k_j-1}(p_j-1) : 1 \le j \le r)$ ~~the divisors of~~ $\cancel{\phi(n) = \prod_{j=1}^{r} p_j^{k_j-1}(p_j-1)}$.

If $k_j > 1$ then $p_j \mid \phi(n)$ but $p_j \nmid n-1$ because $p_j \mid n$.

So $k_j = 1$ $\forall n$. So for a Carmichael number we must have $\phi(n) = \prod_{j=1}^{r} p_j - 1$.

Then $G_n \cong \prod G_{p_j}$. The orders of elements of G_n are all divisors of $\operatorname{lcm}(p_1-1, \dots, p_r-1)$. So every element of G_n has order dividing $n-1 \iff p_j - 1 \mid n-1$ $\forall\ 1 \le j \le r$

72

Corollary of ~~Carmichael~~ Korselt's Criterion — If n is a Carmichael number then n is odd.

Proof: Since n is composite $n = \prod_{j=1}^{r} p_j$ for $r \geq 2$.

So $p_j - 1$ is even for at least one prime p_j

So $p_j - 1 \mid n-1 \Rightarrow n-1$ even $\Rightarrow n$ odd.

The smallest Carmichael number is $561 = 3 \times 11 \times 17$

$560 = 2^4 \times 35 = 2^4 \times 3 \times 5$ $\qquad \phi(561) = 2 \times 10 \times 16 = 320$

~~ϕ lcm $(2,10,16) = 80$ ...~~

$3-1 = 2 \quad 11-1 = 10 \quad 17-1 = 2^4$. All of these divide 560. So 561 is a Carmichael number.

$$\phi(561) = 2 \times 10 \times 16 = 320$$

$$\text{lcm}(2, 10, 16) = 5 \times 2^4 = 80$$

$$x^{80} \equiv 1 \mod 561 \quad \forall\, x \in G_{561}$$

Hence $x^{560} \equiv 1 \mod 561$