MATH 430 Homework 4

Qilin Ye

September 30,2020

Problem 1

Let p be an odd prime and $g \not\equiv 0 \pmod{p}$. Let $q = (p-1)/2$.

(1) What are the possible values that g^q can take?

(2) Suppose further that q is prime. Show that g is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$ unless $g \equiv \pm 1 \pmod{p}$ or $g^q \equiv 1 \pmod{p}$.

Solution

(1) By Fermat's little theorem, we know that (in the group $(\mathbb{Z}/p\mathbb{Z})^*$)

$$(g^q)^2 = g^{p-1} = 1.$$

It immediately follows that g^q can be ± 1 since $(1)^2 = (-1)^2 = 1$. For a more rigorous proof, suppose we have $x^2 \equiv 1 \pmod{p}$, then $x^2 - 1 = (x+1)(x-1) \equiv 0 \pmod{p}$, namely $p \mid (x+1)(x-1)$. It's obvious that, since p is a prime, it either divides $x+1$ or $x-1$, so the only options for x are ± 1 in $\mathbb{Z}/p\mathbb{Z}$. Hence g^q is either 1 or -1.

(2) We already know that $|(\mathbb{Z}/p\mathbb{Z})^*| = p - 1 = 2q$. By Lagrange's theorem, we know that the order of g, $o(g)$, must divide $2q$. Since q is prime, the only divisors — and thus the possible orders of g — are $1, 2, q, 2q$. Since $g \neq 1 \pmod{p}$ we know $g \neq e$ and $o(g) \neq 1$. From part (1) we know that the only possibilities for $o(g)$ to be 2 is if $g = -1$, and this is negated by the problem. We also know $g^q \neq e$ which means $o(g)$ does not divide q; hence it cannot be q. Thus we are left with $o(g) = 2q$, i.e., $\{g, g^2, \ldots, g^{p-1}\}$ contains $p-1$ distinct elements. Since all of these elements need to be in $(\mathbb{Z}/p\mathbb{Z})^*$, and the group has exactly $p-1$ elements, we deduce that $\langle g \rangle = (\mathbb{Z}/p\mathbb{Z})^*$, i.e., g generates $(\mathbb{Z}/p\mathbb{Z})^*$.

Problem 2

Let p be an odd prime and $b \not\equiv 0 \pmod{p}$. Show that the congruence $x^2 \equiv b \pmod{p}$ has 0 solution or 2 solutions mod p (for $0 \leqslant x \leqslant p-1$).

Solution

Notice that if x is a solution to $x^2 \equiv b \pmod{p}$, so is $(-x)$, and they must be distinct because p is odd and $p - x = x$ cannot happen. If we have another y satisfying $y^2 \equiv x^2 \equiv b \pmod{p}$, then $p \mid x^2 - y^2 = (x+y)(x-y)$, and it divides either $x+y$ or $x-y$. Note that since $b \neq 0$ we have $0 < x, y \leqslant p-1$. This means $-(p-1) \leqslant x-y \leqslant p-1$ and $0 < x+y \leqslant 2p-2$. Therefore either $x+y = p$, i.e., $y = -x$, or $x-y = 0$, i.e., $y = x$. We conclude that if $x^2 \equiv b \pmod{p}$ has solutions, it has precisely two solutions. One example is provided in the problem 1 (1).

On the other hand, it is entirely possible that $x^2 = b \pmod{p}$ has no solution: consider the congruence relation $x^2 \equiv 2 \pmod{3}$. A quick test by brute force suggests $1^2 = 1, 2^2 = 1$, and $0^2 = 0$, so no square modulo 3 equals 2.

Problem 3

Let p be an odd prime and let $b \not\equiv 0 \pmod{p}$. Let g be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. Let $b \equiv g^k$ for some $1 \leqslant k \leqslant p-1$. What necessary and sufficient condition can you impose on k so that the congruence $x^2 \equiv b \pmod{p}$ has 2 solutions mod p?

Solution

Since g generates $(\mathbb{Z}/p\mathbb{Z})^*$, if $x^2 \equiv b \pmod{p}$ has solutions, they are of form g^ℓ and $g^{(p-1)-\ell}$ for some ℓ. Then, the original congruence relation becomes (in $\mathbb{Z}/p\mathbb{Z})^*$)

$$g^{2\ell} = g^{2p-2-2\ell} = g^k$$

from which we see 2ℓ, plus or minus any multiples of $(p-1)$, is even. Therefore k being even is a necessary condition in order to make $x^2 \equiv b \pmod{p}$ solvable.

On the other hand, it is sufficient: if k is even then it can be written as $k = 2m$ for some integer m. Then $g^k = (g^m)^2$ and we have found a solution g^m already. The other one will simply be $g^{(p-1)-m}$.

Problem 4

Given 2 is a generator of $(\mathbb{Z}/29\mathbb{Z})^*$, how many generators does this group have? Given 7 is a generator of $(\mathbb{Z}/229\mathbb{Z})^*$, how many generators does this group have?

Solution

(1) Since 2 generates $(\mathbb{Z}/29\mathbb{Z})^*$, we know that

$$\langle 2\rangle = \{\dots, 2^{-2}, 2^{-1}, 1, 2, 2^2, \dots\} = \{1, 2, \dots, 28\},$$

i.e., the set on the LHS permutes the set on the RHS.

First, we claim that $o(2) = 28$. On the one hand, by Lagrange's theorem we immediately know $o(2) \mid |(\mathbb{Z}/29\mathbb{Z})^*| = 28$. On the other hand, if $o(2) < 28$, then the LHS can have at most 27 distinct elements and the equation cannot hold. Hence $o(2) = 28$, i.e., $2^{28} = e$.

Also note that

$$\begin{cases} 2^i 2^j = 2^{i+j} \\ 2^i 2^{28-i} = 2^{28} = e \implies (2^i)^{-1} = 2^{28-i} \end{cases}$$

Now if we only look at the exponents, the two equations give nothing else but the group $(\mathbb{Z}/28\mathbb{Z}, +)$, and the bijective map $f : \mathbb{Z}/28\mathbb{Z} \to (\mathbb{Z}/29\mathbb{Z})^*$ defined by $f(x) = 2^x$ shows that the two groups are isomorphic.

Clearly, as 2 generates $(\mathbb{Z}/29\mathbb{Z})^*$, any other generator (and non-generator) has the form 2^n, and to be a generator, 2^n has to satisfy that, given any b with $0 \leqslant b \leqslant 27$, we can always find an a such that $(2^n)^a = 2^b$ in $\mathbb{Z}/28\mathbb{Z}$. Alternatively, we can write this as

$$an \equiv b \pmod{28}$$

which will always have a solution if and only if $\gcd(n, 28) = 1$. (The "if" part is immediate by applying Euclid's algorithm and solving the equation $b(an) + b(28c) = b(1)$. The "only if" part can be proven by taking the contrapositive: suppose $\gcd(n, 28) = m > 1$, then any $\mathbb{Z}$-combination of n and 28 is still a multiple of m. Hence if $m \nmid b$, it is impossible to find a solution for $an \equiv b \pmod{28}$.)

Therefore, x needs to be coprime with 28 to be a generator of $(\mathbb{Z}/29\mathbb{Z})^*$. Hence there are $\varphi(28) = 28 \cdot (1/2) \cdot (6/7) = 12^\dagger$ such generators.

(2) Likewise, for $(\mathbb{Z}/229\mathbb{Z})^*$, we know it is isomorphic to $(\mathbb{Z}/228\mathbb{Z}, +)$, and the number of generators is $\varphi(228) = 228 \cdot (1/2) \cdot (2/3) \cdot (18/19) = 72^\dagger$.

Remark

In general, $(\mathbb{Z}/m\mathbb{Z})^*$ has $\varphi(m-1)$ generators.

Remark: on Euler's Totient Function

I computed $\varphi(28)$ and $\varphi(228)$ using the following proposition. The screenshot is taken from one of my previous notes.

4.6 Isomorphism and Euler's Totient Function YQL's Notes: Intro to Abstract Algebra

which completes the proof.

Future reference: theorem 4.6.1 □

Problem 4.6.1 (4.6.11)**.** Suppose $n \in \mathbb{Z}^+$ has prime factorization $n = \prod_{i=1}^{s} p_i^{e_i} = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$. Show that

$$\varphi(n) = n \cdot \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right)$$

Solution 4.6.1. Notice that after being prime factorized, n is now expressed as the product of s pairwise co-prime positive integers, each equaling to a prime raised to some positive power. Therefore,

$$\begin{aligned}
\varphi(n) &= \prod_{i=1}^{s} \varphi\left(p_i^{e_i}\right) = \varphi\left(p_1^{e_1}\right) \cdot \varphi\left(p_2^{e_2}\right) \cdots \varphi\left(p_s^{e_s}\right) \\
&= \prod_{i=1}^{s} \left(p_i^{e_i} - p_i^{e_i - 1}\right) = \left(p_1^{e_1} - p_1^{e_1 - 1}\right)\left(p_2^{e_2} - p_2^{e_2 - 1}\right) \cdots \left(p_s^{e_s} - p_s^{e_s - 1}\right) && \text{(by proposition 4.6.10)} \\
&= \prod_{i=1}^{s} \left(p_i^{e_i}\left(1 - \frac{1}{p_i}\right)\right) = \left(p_1^{e_1}\left(1 - \frac{1}{p_1}\right)\right)\left(p_2^{e_1 2}\left(1 - \frac{1}{p_2}\right)\right) \cdots \left(p_s^{e_s}\left(1 - \frac{1}{p_s}\right)\right) \\
&= \left(\prod_{i=1}^{s} p_i^{e_i}\right) \cdot \prod_{i=1}^{s}\left(1 - \frac{1}{p_i}\right) = n \cdot \prod_{i=1}^{s}\left(1 - \frac{1}{p_i}\right)
\end{aligned}$$

Hence proven. □