Random Algebra/Number Theory Problems

Shaun Ostoic

June 11, 2018

Exercise 1. Let G be a finite group. Show that $a \in G$ is a generator of G if and only if $a^{\frac{|G|}{q}} \neq 1$, for each prime factor p of $|G|$.

Proof. ($\Rightarrow$) Since a generates G, it is a cyclic group, hence $G = \langle a \rangle$. A consequence of this is that $|G| = |\langle a \rangle| = |a|$. Let us assume for sake of a contradiction, that $a^{\frac{|G|}{q}} = 1$ for some prime factor q of $|G|$. Then we see that $a^{\frac{|G|}{q}} = 1 \implies |a| \text{ divides } \frac{|G|}{q} \implies |a| = |G| < \frac{|G|}{q}$, which is a contradiction.

($\Leftarrow$) Suppose instead that a is not a generator of G. Then $|a| \neq |G|$, which means there must be a prime divisor q of $|G|$ for which $|a| \text{ divides } \frac{|G|}{q}$. To be more explicit, let us look at the prime factorization of $|G|$ and of $|a|$. Write $|G| = q_1^{g_1} \dots q_r^{g_r}$ and $|a| = q_1^{a_1} \dots q_r^{a_r}$, with $a_i \leq g_i$ for all i. It is entirely possible that a may hold each prime divsior of $|G|$ in its prime factorization, but it does not necessarily have equal exponents in the factorization. Otherwise, $a_i = g_i$ for all i, hence $|a| = |G|$. In this case, $|a|$ and $|G|$ must differ by at least one prime divisor q. Then if we divide out that prime factor from $|G|$, it follows that $|a| \text{ divides } \frac{|G|}{q}$. By one of the previous theorems, this is equivalent to saying that $a^{\frac{|G|}{q}} = 1$, which contradicts the assumption we make in this direction of the proof.

□

Definition (Universal Exponent). A positive integer λ is called the minimal universal exponent if λ is the smallest integer such that $a^\lambda \equiv 1 \mod n$ for all residues a such that $(a, n) = 1$.

Lemma 1. There exists a resiude of order λ, where λ is the minimal universal exponent of p.

Exercise 2. Show that for any prime number $p \geq 3$, $\mathbb{Z}_p^*$ has a primitive root.

Proof. To show that $\mathbb{Z}_p^*$ has a primitive root, it is sufficient to show that $|a| = \phi(p) = p - 1$, for some $a \in \mathbb{Z}_p^*$. Let λ be the minimal universal exponent of p. If $\lambda = p - 1$, then there is a residue of order λ by Lemma (1), hence there is a primitive root. Otherwise, $\lambda < p - 1$. In this case, there are at most λ solutions to the equation $x^\lambda - 1 \equiv 0 \mod p$, by Lagrange's Polynomial Theorem. However, since $a^{p-1} \equiv 1 \mod p$ for all nonzero residues $a \in \mathbb{Z}_p^*$ (due to Fermat's Little Theorem), there are $p - 1 > \lambda$ solutions to the above polynomial, a contradiction. Therefore, $\lambda = p - 1$, which proves there is a resiude of order $\phi(p) = p - 1$, hence there is a primitive root.

□

Exercise 3. Show that a finite subset B of a vector space V over a field F is a basis for V if and only if every $v \in V$ can be written uniquely as a linear combination of vectors from B. That is, where $B = \{b_1, \dots b_n\}$, the scalars $\alpha_i \in F$ for all i are unique for which

$$v = \alpha_1 b_1 + \dots + \alpha_n b_n.$$

Proof. (⇒) Suppose that B is a basis for V. Then B is both a spanning set, and a linearly independent set. It is a spanning set for V, which means that for every $v \in V$, there exist scalars $\alpha_1, \dots \alpha_n \in F$ such that

$$v = \alpha_1 b_1 + \cdots + \alpha_n b_n. \tag{1}$$

B being linearly independent means that if there exist $\eta_1, \dots \eta_n \in F$ such that

$$\eta_1 b_1 + \cdots + \eta_n b_n = 0,$$

then $\eta_i = 0$ for all i.

We must now show that (1) is the only possible way to write v as a linear combination of vectors from B. Suppose for sake of a contradiction that there is another such way to write v, that being

$$v = \beta_1 b_1 + \cdots + \beta_n b_n, \tag{2}$$

where $\beta_1, \dots \beta_n \in F$. Using (1) and (2), we have

$$\beta_1 b_1 + \cdots + \beta_n b_n = \alpha_1 b_1 + \cdots + \alpha_n b_n$$

$$(\alpha_1 - \beta_1) b_1 + \cdots + (\alpha_n - \beta_n) b_n = 0 \tag{3}$$

Let us use the assumption that B is a linearly independent set. Set $\eta_i = (\alpha_i - \beta_i)$ for each i. Then (3) can be written as

$$\eta_1 b_1 + \cdots + \eta_n b_n = 0,$$

which implies that $\eta_i = 0$ for all i by linear independence of B. That is, $\alpha_i - \beta_i = 0$, hence $\alpha_i = \beta_i$ for all i, which proves that these two ways of writing v are the same.

(⇐) Suppose that every $v \in V$ can be written uniquely as a linear combination of vectors from B. We must show that B is both a linearly independent set, and a spanning set for V. First we show that it is a spanning set. Given any $v \in V$, by assumption we can write

$$v = \alpha_1 b_1 + \cdots + \alpha_n b_n,$$

for some scalars $\alpha_1, \dots \alpha_n \in F$. We are done since this is the definition of B being a spanning set for V. Last, to show that it is linearly independent, suppose there exist $\alpha_i \dots \alpha_n \in F$, such that

$$\alpha_1 b_1 + \cdots + \alpha_n b_n = 0.$$

This is also saying that

$$\alpha_1 b_1 + \cdots + \alpha_n b_n = 0 \cdot b_1 + \cdots + 0 \cdot b_n,$$

which implies that $\alpha_i = 0$ for all i. This is because we've assumed that there is only one such way to write this linear combination of vectors, hence B must be linearly independent. Therefore, B is a basis for V. □

Exercise 4. Let p be an odd prime and let $k \geq 1$.

1. a is an odd primitive root modulo $p^k \implies a$ is a primitive root modulo $2p^k$.
2. a is an even primitive root modulo $p^k \implies a + p^k$ is a primitive root modulo $2p^k$.

Proof. (1) Assume a is an odd primitive root modulo p^k. Then $\phi(2p^k) = \phi(2)\phi(p^k) = \phi(p^k)$. Suppose for sake of a contradiction that $|a| < \phi(2p^k)$, and let $m = |a|$. Then $a^m \equiv 1 \mod 2p^k$, hence $a^m - 1 = 2p^k\ell$ for some ℓ. If we bring the equation back into $\mathbb{Z}_p^*$, we have $a^m \equiv 1 \mod p^k$. However, we know that a is a primitive root modulo p^k, so this contradicts the order of a being $\phi(p^k)$. Thus, $|a| = \phi(2p^k)$, which means a is also a primitive root modulo $2p^k$.

(2) Assume that a is an even primitive root modulo p^k. To prove $a + p^k$ is a primitive root modulo $2p^k$, assume it is not, for sake of a contradiction. Let $m = |a + p^k| < \phi(2p^k)$, which leaves us with the congruences

$$(a + p^k)^m \equiv 1 \mod 2p^k,$$
$$(a + p^k)^m - 1 = 2p^k\ell,$$
$$(a + p^k)^m \equiv 1 \mod p^k,$$

for some ℓ. Observe by properties of congruences that

$$a + p^k \equiv a \mod p^k \implies (a + p^k)^m \equiv a^m \mod p^k.$$

Using the same technique as in (1) together with this observation yields $a^m \equiv 1 \mod p^k$, where $m < \phi(p^k)$. We initially assumed that a is a primitive root, meaning $|a| = \phi(p^k)$, which is contradicted by this new deduction. Therefore, $a + p^k$ must be a primitive root modulo $2p^k$. □

Exercise 5. Let p be an odd prime number, and let $a \in \mathbb{Z}_p^*$. Show that $|a| = q$, where q is a divisor of $p - 1$, if and only if

1. $a^q \equiv 1 \mod p$
2. $a^{\frac{q}{r}} \equiv 1 \mod p$,

where r is any prime divisor of q.

Proof. □

Exercise 8. Define the concept of primitive root modulo p, where p is a prime number.

Solution. A primitive root a modulo p is an element $a \in \mathbb{Z}_p^*$ such that $|a| = \phi(p)$. Equivalently, a primitive root a modulo p is an element such that every residue $b \in \mathbb{Z}_p^*$ can be written as $b \equiv a^k \mod p$ for some $k \in \mathbb{Z}$. □

Exercise 9. content...

Exercise 9. Let $p = 4q+1$ be a prime number, where q is an odd prime. Show that 2 is a primitive root modulo p.

Proof. Suppose 2 is not a primitive root modulo p, and let $m = |2|$. Then $2^m \equiv 1 \mod p$, meaning $2^m - 1 = (4q + 1)\ell$, for some ℓ.

Let g be a primitive root modulo p, and write $2 = g^i$ for some i.

$$2^m - 1 = 4q\ell + \ell$$

$$|2^{\frac{p-1}{2}}| = \frac{|2|}{(\frac{p-1}{2}, |2|)}$$

$$|2|(\frac{p-1}{2}, |2|) = 2$$

TODO: □

Exercise 10. Discuss $\mathbb{Z}_m$, for a positive integer m.

Solution. For an arbitrary positive integer m, not every residue modulo m has an inverse, which is a desirable property for many applications. As such, finding a criterion for which $\mathbb{Z}_m$ contains multiplicative inverses for each nonzero residue is an important venture. In general, any residue $a \in \mathbb{Z}_m$ has a multiplicative inverse provided that $(a, m) = 1$, and vice versa. From this point, one might ask what a residue system in which every nonzero residue has a multiplicative inverse. That is, given any residue a, suppose $(a, m) = 1$. The only such integers m for which $(a, m) = 1$for all $a < m$ are the prime numbers. Thus, a residue system $\mathbb{Z}_m$ is "complete", is a "field", contains multiplicative inverses, etc, if and only if m is prime. □

Exercise 12. Define the characteristic of a ring R.

Solution. Given a unital ring R (a ring with 1), the characteristic n is the smallest positive integer such that $1 + 1 + \cdots + 1 = 0$ (n times). That is, such that $\sum_{i=1}^{n} 1 = 0$. □

Lemma 2. Let g be a primitive root modulo p, let a be a residue modulo p, and write $a = g^i$ for some i.

1. a is a quadratic residue modulo $p \iff i$ is even .
2. a is a nonquadratic residue modulo $p \iff i$ is odd

Exercise 13. Let p be a prime number.

1. a and b are quadratic residues modulo $p \implies ab$ is a quadratic residue modulo p.
2. a is a quadratic residue and b is a nonquadratic residue $\implies ab$ is a nonquadratic residue modulo p.
3. a and b are both nonquadratic residues modulo $p \implies ab$ is a quadratic residue modulo p.

Proof. (1) Suppose both a and b are quadratic residues modulo p. Then by Lemma 2 above, we can write $a \equiv g^{2i}$ and $b \equiv g^{2j}$ for some i and j, and where g is a primitive root modulo p. It follows that $ab \equiv g^{2i}g^{2j} \equiv g^{2(i+j)}$, hence ab is a primitive root by the lemma.

(2) Assume a is a quadratic residue, and b is a nonquadratic residue modulo p. By the lemma, we can write $a \equiv g^{2i}$ and $b \equiv g^{2j+1}$, for some i, j. Similar to before, we see that $ab \equiv g^{2i}g^{2j+1} =\equiv g^{2(i+j)+1}$, hence ab is a nonquadratic residue modulo p.

(3) Lastly, assume both a and b are nonquadratic residues modulo p. Writing $a \equiv g^{2i+1}$ and $b \equiv g^{2j+1}$, we see that $ab \equiv g^{2i+1}g^{2j+1} \equiv g^{2(i+j)+2} \equiv g^{2(i+j+1)}$. Thus, ab is a quadratic residue modulo p. □