Peize Liu
St. Peter's College
University of Oxford

Problem Sheet 2

ASO: Number Theory

May 19, 2020

Question 1

Suppose that p and $q = 2p + 1$ are both odd primes. Explain why (a) $2p$ is a quadratic non-residue of q and (b) q has $p - 1$ primitive roots.

Show that the primitive roots of q are precisely the quadratic non-residues of q, other than $2p$.

Proof. (a) We have $2p \equiv -1 \pmod{q}$. By Corollary 4.1, $2p$ is a quadratic residue and q if and only if $q \equiv 1 \pmod{4}$. But since p is an odd prime, $p = 2k + 1$ for some $k \in \mathbb{Z}$. Then $q = 4k + 3 \equiv 3 \pmod{4}$. Hence $2p$ is a quadratic non-residue of q.

(b) Since q is prime, $(\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic. In particular we have

$$(\mathbb{Z}/q\mathbb{Z})^\times \cong C_{q-1} = C_{2p} \cong C_2 \times C_p.$$

by Chinese Remainder Theorem. We note that $(1, g)$ is a generator of $C_2 \times C_p$ for $g \neq 0$. Hence $C_2 \times C_p$ has $p - 1$ elements of order $2p$. It follows that q has $p - 1$ primitive roots.

Let $\sigma : (\mathbb{Z}/q\mathbb{Z})^\times \to C_2 \times C_p$ be an group isomorphism. As $\{0\} \times C_p$ is a normal subgroup of $C_2 \times C_p$ of index 2, it follows that $\sigma^{-1}(\{0\} \times C_p)$ is precisely the subgroup of quadratic residues in $(\mathbb{Z}/q\mathbb{Z})^\times$. Then the quadratic non-residues of $(\mathbb{Z}/q\mathbb{Z})^\times$ hace image $\{1\} \times C_p$ under σ. As we have shown in (b), $\{1\} \times C_p \backslash \{0\}$ corresponds to the set of primitive roots of q. The remaining element $(1, 0) \in C_2 \times C_p$ is the unique element in $C_2 \times C_p$ of order 2. And we note that $2p \equiv -1 \pmod{q}$ is of order 2. We then conclude that $\sigma^{-1}((1, 0)) = 2p$. □

Simpler to compute $\phi(q-1)$

Question 2

Prove that if n has a primitive root then it has $\phi(\phi(n))$ of them.

Proof. Suppose that n has a primitive root. Then the muliplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ has an element of order $n - 1$. It follows that $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic. Let $\phi(n) = m$. Then $(\mathbb{Z}/n\mathbb{Z})^\times \cong C_m \cong \mathbb{Z}/m\mathbb{Z}$. In addition, we know that $k \in \mathbb{Z}/m\mathbb{Z}$ generates $\mathbb{Z}/m\mathbb{Z}$ if and only if $\gcd(m, k) = 1$. Therefore $\mathbb{Z}/m\mathbb{Z}$ has $\phi(m)$ generators, each corresponding to a primitive root of n. We conclude that n has $\phi(\phi(n))$ primitive roots. □

Question 3

Let p be an odd prime. Show that every element in $\mathbb{Z}/p\mathbb{Z}$ can be written as the sum of two squares.

Proof. Since p is an odd prime, $p = 2k+1$ for some $k \in \mathbb{N}$. It follows that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic and $(\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1} = C_{2k} \cong C_2 \times C_k$. The quadratic residues of p forms a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ of index 2, which means that there are k of them. We have:

$$\operatorname{card}\{a^2 : a \in \mathbb{Z}/p\mathbb{Z}\} = k + 1.$$

For $m \in \mathbb{Z}/p\mathbb{Z}$, suppose that m is not the sum of two squares. Then $m - a^2$ is a quadratic non-residue for each $a \in \mathbb{Z}/p\mathbb{Z}$. But

$$\operatorname{card}\{m - a^2 : a \in \mathbb{Z}/p\mathbb{Z}\} = \operatorname{card}\{a^2 : a \in \mathbb{Z}/p\mathbb{Z}\} = k + 1.$$

It follows that $\mathbb{Z}/p\mathbb{Z}$ has at least $k + 1$ quadratic non-residues, which is a contradication, as the number of quadratic residues and non-residues are equal. □

Question 4

Do there exist integer solutions to the equation $x^2 \equiv 251 \pmod{779}$? *Note that* $779 = 19 \times 41$.

Solution. Since $779 = 19 \times 41$ and 19 is coprime with 41, by Chinese Remainder Theorem we have $C_{779} = C_{19} \times C_{41}$.

Note that $251 = 19 \times 13 + 4 = 41 \times 6 + 5$. By Chinese Remainder Theorem,

$$x^2 \equiv 251 \pmod{779} \iff x^2 \equiv 4 \pmod{19} \wedge x^2 \equiv 5 \pmod{41}$$

We can check that whether 4 is a quadratic residue of 19 and whether 5 is a quadratic residue of 41 by the proceduce described in Example 4.1.

Since $19 \equiv 4 \equiv 3 \pmod{4}$, by Law of Quadratic Reciprocity, $\left(\frac{4}{41}\right) = -\left(\frac{19}{4}\right) = -\left(\frac{3}{4}\right)$. It is obvious that 3 is a quadratic non-residue of 4, it follows that 4 is a quadratic residue of 19.

Since $41 \equiv 1 \pmod{4}$, by Law of Quadratic Reciprocity, $\left(\frac{5}{41}\right) = \left(\frac{41}{5}\right) = \left(\frac{1}{5}\right)$. It is obvious that 1 is a quadratic residue of 5, it follows that 5 is a quadratic residue of 41.

We conclude that 251 is a quadratic residue of 779. There exists $x \in \mathbb{Z}$ such that $x^2 \equiv 251 \pmod{779}$. □

Question 5

Does the equation $x^2 + 10x + 15 \equiv 0 \pmod{45083}$ have any integer solutions? *Note that* 45083 *is prime.*

Solution. Note that $x^2 + 10 + 15 = (x+5)^2 - 10$. Then

$$x^2 + 10x + 15 \equiv 0 \pmod{45083} \iff (x+5)^2 \equiv 10 \pmod{45083}$$

The existence of the solutions is equivalent to that 10 is a quadratic residue of 45083.

Since $10 \equiv 2 \pmod{4}$, by the Law of Quadratic Reciprocity,

$$\left(\frac{10}{45083}\right) = \left(\frac{45083}{10}\right) = \left(\frac{3}{10}\right) = \left(\frac{10}{3}\right) = \left(\frac{1}{3}\right).$$

It is obvious that 1 is a quadratic residue of 3. Then 10 is a quadratic residue of 45083. We conclude that $x^2 + 10x + 15 \equiv 0 \pmod{45083}$ has integer solutions. □

Question 6

Use the Fermat method to factorise 9579, without using a calculator.

Solution. We shall first find the least perfect square bigger then 9579. Note that $90^2 = 8100 < 9579 < 10000 = 100^2$. We use binary search and try $95^2 = 9025$. Next we try $97^2 = (95+2)^2 = 9025 + 4 \times 96 = 9409$. It is already very closed to 9579. Next we try $98^2 = (97+1)^2 = 9409 + 97 + 98 = 9604 > 9579$.

It happens that $98^2 - 9579 = 25 = 5^2$, which is the number we are looking for. We immediately have $9579 = 98^2 - 5^2 = 93 \times 103 = 3 \times 31 \times 103$. This gives the complete factorization of 9579. □

Remark. The easiest way of factorizing 9579 is as follows. First we note that $9+5+7+9 = 30$ is divisible by 3. Hence we obtain $9579 = 3 \times 3193$. But it is obvious that 3193 is divisible by 31. We obtain the complete factorization: $9579 = 3 \times 31 \times 103$.

Question 7

For any integer $n \geqslant 2$, let $F_n = 2^{2^n} + 1$ be the n-th "Fermat number". Suppose that p is a prime factor of F_n.

(i) Show that $\operatorname{ord}_p(2) = 2^{n+1}$.

(ii) Show that $2^{(p-1)/2} \equiv 1 \pmod{p}$.

(iii) Deduce that $p = 1 + 2^{n+2}k$ for some $k \in \mathbb{N}$.

Hence, or otherwise, verify that $F_4 = 65537$ is prime.

Proof. (i) We have $2^{2^n} \equiv -1 \pmod{F_n}$. Since $p \mid F_n$, $2^{2^n} \equiv -1 \pmod{p}$. Then $\left(2^{2^n}\right)^2 = 2^{2^{n+1}} \equiv 1 \pmod{F_n}$. We have $\operatorname{ord}_p(2) \mid 2^{n+1}$. If $\operatorname{ord}_p(2) < 2^{n+1}$, then $\operatorname{ord}_p(2) \mid 2^n$, which is contradictory. We conclude that $\operatorname{ord}_p(2) = 2^{n+1}$.

(ii) By Lagrange Theorm, $\operatorname{ord}_p(2) \mid |(\mathbb{Z}/p\mathbb{Z})^\times|$. Since p is a odd prime, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic and has order $p-1$. Therefore $2^{n+1} \mid p-1$. Since $n \geqslant 2$, we have $p \equiv 1 \pmod{8}$. By Proposition 4.2, 2 is a quadratic residue of p. By Euler's criterion, $2^{(p-1)/2} \equiv 1 \pmod{p}$.

(iii) Since $2^{(p-1)/2} \equiv 1 \pmod{p}$ and $\operatorname{ord}_p(2) = 2^{n+1}$, we have $2^{n+1} \left| \frac{p-1}{2} \right.$. Both sides are positive integers, there exists $k \in \mathbb{Z}_+$ such that $\frac{p-1}{2} = 2^{n+1}k$. Hence $p = 1 + 2^{n+2}k$.

For $n = 4$, $p = 1 + 2^6 k = 1 + 64k$. Suppose that $F_4 = pq$. We have

$$1 \equiv F_4 = (1 + 64k)q = q + 64kq \equiv q \pmod{64}.$$

Then there exists $l \in \mathbb{N}$ such that $q = 1 + 64l$.

$$F_4 = 2^{16} + 1 = (1 + 2^6 k)(1 + 2^6 l) = 1 + 2^6(k + l) + 2^{12}kl \implies 2^{10} = 2^6 kl + k + l.$$

As $k + l > 0$, we have $2^{10} > 2^6 kl$. So $kl < 16$. If $l > 0$, then $k < 16$ and $k < 16$. It follows that $0 < k + l < 32$. However, $2^{10} = 2^6 kl + k + l$ implies that $k + l \equiv 0 \pmod{64}$, which is a contradiction. Hence $l = 0$ and $k = 2^10$. We conclude that $p = 1 + 2^6 \times 2^{10} = F_4$ and F_4 is prime. □

Question 8

Using the Fermat method, factorise 2881, and hence find $\phi(2881)$.

A message has been encrypted using RSA and the encoding $01 \leftrightarrow A$, $02 \leftrightarrow B$, $03 \leftrightarrow C$, etc. with exponent $e = 5$ and modulus $n = 2881$. The message is 2352 2138 0828. What is the plain text message? *I suggest using a free online modular exponentation calculator, which you can find by a google search for those terms.*

Solution. Since $50^2 = 2500 < 2881 < 60^2 = 3600$, first we try $55^2 = 3025$. $3025 - 2881 = 144 = 12^2$. We find the factorization: $2881 = 55^2 - 12^2 = 43 \times 67$. Then $\phi(2881) = (43 - 1)(67 - 1) = 2772$.

Next we shall find $d \in \mathbb{Z}$ such that $de \equiv 1 \pmod{2772}$. By Euclidean Algorithm:

$$2772 = 554 \times 5 + 2$$
$$5 = 2 \times 2 + 1$$

Hence $1 = 5 - 2 \times 2 = 5 - 2 \times (2772 - 554 \times 5) = -2 \times 2772 + 1109 \times 5$. We can set $d = 1109$ so that $de \equiv 1 \pmod{2772}$.

Next we compute the following expressions using modular exponential calculator:

$$2352^{1109} \equiv 1524 \pmod{2881} \qquad 2138^{1109} \equiv 615 \pmod{2881} \qquad 828^{1109} \equiv 1804 \pmod{2881}.$$

Then the decrypted message is 1524 0615 1804, which translates to "OXFORD" in plain English. □

Question 9

Let $p \geqslant 7$ be a prime. Show that every non-zero element of $\mathbb{Z}/p\mathbb{Z}$ is a sum of two *non-zero* squares.

Proof. Note that $3, 4, 5$ are a Pythagorean triple: $3^2 + 4^2 = 5^2$.

bad notation

Since $p \geqslant 7$ is prime, p is coprime with 3, 4, and 5. In particular, $5^{-1} \in \mathbb{Z}/p\mathbb{Z}$. For nonzero $a \in \mathbb{Z}/p\mathbb{Z}$, we have

$$a^2 = \left(\frac{3}{5}a\right)^2 + \left(\frac{4}{5}a\right)^2$$

where $\frac{3}{5}a$ and $\frac{4}{5}a$ are both non-zero in $\mathbb{Z}/p\mathbb{Z}$. We conclude that all non-elements of $\mathbb{Z}/p\mathbb{Z}$ is a sum of two non-zero squares. □

What about non-squares $b \neq a^2$?