Math 261 — Exercise sheet 5

http://staff.aub.edu.lb/~nm116/teaching/2017/math261/index.html

Version: October 23, 2017

Answers are due for Monday 23 October, 11AM.

The use of calculators is allowed.

Exercise 5.1: $\sqrt[67]{2} \bmod 101$ (10 pts)

How many elements $x \in \mathbb{Z}/101\mathbb{Z}$ satisfy $x^{67} = 2$? Compute them.

Note: 101 is prime.

Solution 5.1:

Since 67 is coprime to $101 - 1 = 100$, the map

$$\begin{array}{ccc} (\mathbb{Z}/101\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/101\mathbb{Z})^\times \\ x & \longmapsto & x^{67} \end{array}$$

is 1-to-1. In particular, there is a unique x such that $x^{67} = 2$, and it is given by the formula $x = 2^{67^{-1}}$, where 67^{-1} denotes the inverse of 67 mod 100. We compute that $100 = 67 + 33$, and $67 = 2 \times 33 + 1$, whence $67 \times 3 - 2 \times 100 = 1$ so $67^{-1} = 3$, so the value of this x is

$$x = 2^3 = 8.$$

Exercise 5.2: Legendre symbols (21 pts)

Compute the following Legendre symbols (7 pts each):

1. $\left(\dfrac{10}{1009}\right)$,
2. $\left(\dfrac{261}{2017}\right)$,
3. $\left(\dfrac{-77}{9907}\right)$.

Note: 1009, 2017 and 9907 are prime.

Solution 5.2:

1. $\left(\frac{10}{1009}\right) = \left(\frac{2}{1009}\right)\left(\frac{5}{1009}\right) = +1 \times + \left(\frac{1009}{5}\right)$

   since $1009 \equiv 1 \pmod 8$ and 1009 (or 5) $\equiv +1 \pmod 4$

   $= \left(\frac{9}{5}\right) = +1$

   since $1009 \equiv 9 \pmod 5$ and 9 is obviously a square mod 5.

2. $\left(\frac{261}{2017}\right) = \left(\frac{3^2}{2017}\right)\left(\frac{29}{2017}\right) = +1 \times + \left(\frac{2017}{29}\right)$

   since 3^2 is obviously a square and since 2017 (or 29) $\equiv +1 \pmod 4$

   $= \left(\frac{16}{29}\right) = +1$

   since $2017 \equiv 16 = 4^2 \pmod{29}$.

3. $\left(\frac{-253}{9923}\right) = \left(\frac{-1}{9923}\right)\left(\frac{11}{9923}\right)\left(\frac{23}{9923}\right) = -1 \times - \left(\frac{9923}{11}\right) \times - \left(\frac{9923}{23}\right)$

   since $253 = 11 \times 23$ and 9923, 11 and 23 are all $\equiv -1 \pmod 4$

   $= - \left(\frac{1}{11}\right)\left(\frac{11 \times 30^2}{23}\right)$

   since $9923 \equiv 1 \pmod{11}$ and $9923 \equiv 9900 = 11 \times 30^2 \pmod{23}$

   $= - \left(\frac{11}{23}\right) = - - \left(\frac{23}{11}\right)$

   since 11 and 23 are both $\equiv -1 \pmod 4$

   $= \left(\frac{1}{11}\right) = +1.$

Exercise 5.3: Quadratic equations mod 55 (21 pts)

Use the Chinese remainders theorem and Legendre symbols to determine the number of solutions in $\mathbb{Z}/55\mathbb{Z}$ to these equations (7 pts each):

1. $x^2 - x + 8 = 0$,
2. $x^2 + 3x + 7 = 0$,
3. $x^2 - 4x - 1 = 0$.

Note: 55 is ***NOT*** *prime.*

Solution 5.3:

Since 5 and 11 are coprime, by CRT we have a 1-to-1 correspondence

$$\mathbb{Z}/55\mathbb{Z} \longleftrightarrow \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z},$$

so that for each equation, the number of solutions in $\mathbb{Z}/55\mathbb{Z}$ is the product of the number of solutions in $\mathbb{Z}/5\mathbb{Z}$ and of that of solutions in $\mathbb{Z}/11\mathbb{Z}$. These numbers are in turn determined by the "quadratic residue-ness" of the discriminant of the equation.

1. The discriminant is $\Delta = 1 - 4 \times 8 = -31$. We have $\left(\frac{\Delta}{5}\right) = \left(\frac{-1}{5}\right) = +1$, whence 2 solutions in $\mathbb{Z}/5\mathbb{Z}$, but $\left(\frac{\Delta}{11}\right) = \left(\frac{2}{11}\right) = -1$, whence no solutions in $\mathbb{Z}/11\mathbb{Z}$. So no solutions in $\mathbb{Z}/55\mathbb{Z}$.

2. This time the discriminant is $\Delta = -19$, and we have $\left(\frac{\Delta}{5}\right) = \left(\frac{\Delta}{11}\right) = +1$, whence 2 solutions in $\mathbb{Z}/5\mathbb{Z}$ and 2 solutions in $\mathbb{Z}/11\mathbb{Z}$, so 4 solutions in $\mathbb{Z}/55\mathbb{Z}$.

3. This time the discriminant is $\Delta = 20$, and we have $\left(\frac{\Delta}{5}\right) = 0$, whence 1 solution in $\mathbb{Z}/5\mathbb{Z}$, and $\left(\frac{\Delta}{11}\right) = +1$, whence 2 solutions in $\mathbb{Z}/11\mathbb{Z}$. So we have 2 solutions in $\mathbb{Z}/55\mathbb{Z}$.

Exercise 5.4: Applications of $\left(\frac{-3}{p}\right)$ (26 pts)

1. (6 pts) Let $p > 3$ be a prime. Prove that -3 is a square mod p if and only if $p \equiv 1 \pmod 6$.

2. (8 pts) An element $x \in \mathbb{Z}/p\mathbb{Z}$ is called a *cubic root of unity* if it satisfies $x^3 = 1$. Use the previous question and the identity $x^3 - 1 = (x-1)(x^2 - x + 1)$ to compute the number of cubic roots of unity in $\mathbb{Z}/p\mathbb{Z}$ in terms of p mod 6.

3. (8 pts) Find another way to compute the number of cubic roots of unity in $\mathbb{Z}/p\mathbb{Z}$ in terms of p mod 6 by considering the map

$$\begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \\ x & \longmapsto & x^3. \end{array}$$

4. (4 pts) Use question 1. of this exercise to prove that there are infinitely many primes p such that $p \equiv 1 \pmod 6$.

   Hint: Suppose on the contrary that there are finitely many, say $p_1, \cdots, p_k$, and consider $N = 12(p_1 \cdots p_k)^2 + 1$.

Solution 5.4:

1. We compute that

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{p'}(-1)^{\frac{3-1}{2}p'}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

   Besides, as $p > 3$, we know that $p \equiv \pm 1 \pmod 6$. So if $p \equiv +1 \pmod 6$, then $p \equiv +1 \pmod 3$, so $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = +1$, but if $p \equiv -1 \pmod 6$, then $p \equiv -1 \pmod 3$, so $\left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1$ since $3 \equiv -1 \pmod 4$.

2. Cubic roots of unity are by definition the same as the roots of the polynomial $x^3 - 1 = (x-1)(x^2 - x + 1)$. The factor $x - 1$ gives the obvious root $x = 1$. Also, the discriminant of $x^2 - x + 1$ is $\Delta = -3$, so by the previous question this factor has 2 distinct roots when $p \equiv +1 \pmod 6$, and 0 roots when $p \equiv -1 \pmod 6$. Besides, these roots can never be $x = 1$, since $x^2 - x + 1$ assumes the value 1 at $x = 1$, and $1 \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$ for all p.

   Thus the number of cubic roots of unity in $\mathbb{Z}/p\mathbb{Z}$ is $1 + 2 = 3$ when $p \equiv +1 \pmod 6$, and $1 + 0 = 1$ when $p \equiv -1 \pmod 6$.

3. If $p \equiv +1 \pmod 6$, then $6 \mid (p-1)$, so $\gcd(3, p-1) = 3$, which means that the map

$$\begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \\ x & \longmapsto & x^3 \end{array}$$

   is 3-to-1. Since 1 is clearly in its image (it is reached by $x = 1$), it is reached by exactly 3 values of x; in other words, there are 3 cubic roots of unity.

   On the other hand, if $p \equiv -1 \pmod 6$, then $\gcd(3, p-1) = 1$, so the map

$$\begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \\ x & \longmapsto & x^3 \end{array}$$

   is 1-to-1, so it assumes the value 1 exactly once, so there is 1 cubic root of unity.

4. Let us suppose that $p_1, \cdots, p_k$ are all the primes $\equiv +1 \pmod 6$, let $N = 12(p_1 \cdots p_k)^2 + 1$, and let p be a prime dividing N (which exists since obviously $N > 1$). Then p cannot be 2, nor 3, nor any of the $p_1, \cdots, p_k$, for else it would divide 1. So we must have $p \equiv -1 \pmod 6$. But since $p \mid N$, we have $-1 \equiv 12(p_1 \cdots p_k)^2 \pmod p$, so $-3 \equiv 36(p_1 \cdots p_k)^2 = (6p_1 \cdots p_k)^2$ is a square mod p, which contradicts question 1.

Exercise 5.5: Pépin's test (22 pts)

Recall (cf sheet 1 exercise 4) that the n-th Fermat number is $F_n = 2^{2^n} + 1$, where $n \in \mathbb{N}$.

1. (2 pts) Prove that $F_n \equiv -1 \pmod 3$.

2. (10 pts) Prove that if F_n is prime, then $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.

3. (10 pts) Conversely, prove that if $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$, then F_n is prime. *Hint: what can you say about the multiplicative order of* $3 \bmod F_n$*?*

Remark: This primality test, named after the 19th century French mathematician Théophile Pépin, only applies to Fermat numbers, but is much faster than the general-purpose tests that can deal with any integer. It was used in 1999 to prove that F_{24} is composite, which is quite an impressive feat since F_{24} has 5050446 digits!

Solution 5.5:

1. Since $2 \equiv -1 \pmod 3$, we have
$$F_n = 2^{2^n} + 1 \equiv (-1)^{2^n} + 1 = 1 + 1 = 2 \equiv -1 \pmod 3$$
as $n \geqslant 1$.

2. If $F_n = p$ is prime, then we have $3^{(F_n-1)/2} = 3^{p'} \equiv \left(\frac{3}{p}\right) \pmod p$, and $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ by quadratic reciprocity since clearly $p = F_n \equiv 1 \pmod 4$. Finally, by the previous question $\left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1$, whence the result.

3. If $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$, then $3^{F_n-1} \equiv (-1)^2 = 1 \pmod{F_n}$, so the multiplicative order of 3 mod F_n divides $F_n - 1 = 2^{2^n}$, which is a power of 2. Since $3^{(F_n-1)/2} \equiv -1 \not\equiv 1 \pmod{F_n}$, and since 2 is the only prime dividing $F_n - 1$, this order is in fact exactly $F_n - 1$. So the powers of 3 give us $F_n - 1$ elements in $(\mathbb{Z}/F_n\mathbb{Z})^\times$. But the number of elements in $(\mathbb{Z}/F_n\mathbb{Z})^\times$ is at most $F_n - 1$ since 0 is not invertible, so the powers of 3 give us all of $(\mathbb{Z}/F_n\mathbb{Z})^\times$ (i.e. 3 is a primitive root mod F_n) and all nonzero elements in $\mathbb{Z}/F_n\mathbb{Z}$ are invertible. This means that $\mathbb{Z}/F_n\mathbb{Z}$ is a field, which implies that F_n is prime.

The exercises below are not mandatory. They are not worth any points, and are given here for you to practise. The solutions will be made available with the solutions to the other exercises.

Exercise 5.6: Sums of Legendre symbols

Let $p \in \mathbb{N}$ be an odd prime.

1. Compute $\displaystyle\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x}{p}\right)$.

2. Compute $\displaystyle\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right)$.

   Hint: write $x(x+1) = x^2(1 + \frac{1}{x})$ wherever legitimate.

Solution 5.6:

1. In $\mathbb{Z}/p\mathbb{Z}$, we have one zero, p' nonzero squares, and p' nonzero nonsquares, so this sum is
$$0 + p' - p' = 0.$$

2. We compute
$$\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right) = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x(x+1)}{p}\right) = \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{x(x+1)}{p}\right)$$
since the term for $x = 0$ is 0
$$= \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{x^2(1+1/x)}{p}\right) = \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{1+1/x}{p}\right) = \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{1+x}{p}\right)$$

since the map $x \mapsto 1/x$ induces a permutation of $(\mathbb{Z}/p\mathbb{Z})^\times$

$$= \sum_{\substack{x \in \mathbb{Z}/p\mathbb{Z} \\ x \neq 1}} \left(\frac{x}{p}\right) = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x}{p}\right) - \left(\frac{1}{p}\right) = 0 - 1 = -1$$

by the previous question.

Remark: If we fix p and take $x \in \mathbb{Z}/p\mathbb{Z}$ uniformly at random, the first formula tells us that the expected value of $\left(\frac{x}{p}\right)$ is 0, and the second one that the covariance of $\left(\frac{x+1}{p}\right)$ and of $\left(\frac{x}{p}\right)$ is $-\frac{1}{p}$. This means that for large p, the value of $\left(\frac{x+1}{p}\right)$ is approximately independent of that of $\left(\frac{x}{p}\right)$.

Exercise 5.7: A test for higher powers

Let $p \in \mathbb{N}$ be a prime, $k \in \mathbb{N}$ be an integer, $g = \gcd(p-1, k)$, and $p_1 = (p-1)/g \in \mathbb{N}$. Finally, let $x \in (\mathbb{Z}/p\mathbb{Z})^\times$.

1. Prove that x is a k-th power if and only if $x^{p_1} = 1$.
2. (Application) Is 2 a cube in $\mathbb{Z}/13\mathbb{Z}$? What about 5?
3. For general x, what kind of number is x^{p_1}, i.e. which equation does it satisfy?
4. Use the above to define a generalization of the Legendre symbol, and state a couple of its properties.

Solution 5.7:

1. Suppose that $x = y^k$ is a k-th power. Then we have $x^{p_1} = y^{kp_1} = y^{\frac{k}{g}(p-1)} = 1$ by Fermat's little theorem.

   So every k-th power is a root of the polynomial $x^{p_1} - 1$. This polynomial has degree p_1, so it has at most p_1 roots; on the other hand, we know that one in g elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ is a k-th power, so there are $(p-1)/g = p_1$ k-th powers, all of which are roots of $x^{p_1} - 1$ by the above. Thus the roots of $x^{p_1} - 1$ are exactly the k-th powers, whence the result.

2. We take $p = 13$, $k = 3$, so $p_1 = 4$.

   We have $2^{p_1} = 16 \equiv 3 \not\equiv 1 \pmod{13}$, so 2 is not a cube mod 13, but $5^{p_1} \equiv 1 \pmod{13}$, so 5 is a cube mod 13 (and it has $g = 3$ cubic roots in $\mathbb{Z}/13\mathbb{Z}$).

3. By Fermat's little theorem, we have

   $$1 = x^{p-1} = x^{p_1 g} = (x^{p_1})^g.$$

   So the number $y = x^{p_1}$ always satisfies $y^g = 1$; in more pedant terms, it is a g-th root of unity.

4. We are thus led to defining $\left(\frac{x}{p}\right)_k = x^{p_1}$.

We have

$$\left(\frac{x}{p}\right)_k = \begin{cases} 0, & \text{if } x = 0, \\ 1, & \text{if } x \text{ is a nonzero } k\text{-th power}, \\ \text{another } g\text{-th root of unity}, & \text{else.} \end{cases}$$

Besides, it follows immediately from the definition that $\left(\frac{xy}{p}\right)_k = \left(\frac{x}{p}\right)_k \left(\frac{y}{p}\right)_k$ for all $x, y \in \mathbb{Z}/p\mathbb{Z}$, and that $\left(\frac{-1}{p}\right)_k = (-1)^{p_1}$.

Remark: In order to make this generalization of the Legendre symbol really practical, we need a generalization of the quadratic reciprocity law. Such a generalization exists, and is a consequence of the more general Artin reciprocity law*, which stands at the pinnacle of 20th century number theory, but is unfortunately far beyond the scope of this course.*