Math 261 — Exercise sheet 7

http://staff.aub.edu.lb/~nm116/teaching/2018/math261/index.html

Version: November 7, 2018

Answers are due for Wednesday 7 November, 11AM.

The use of calculators is allowed.

Exercise 7.1: Legendre symbols (30 pts)

Compute the following Legendre symbols (10 pts each):

1. $\left(\frac{-6}{10007}\right)$,
2. $\left(\frac{261}{2903}\right)$,
3. $\left(\frac{8000}{29}\right)$.

Note: 10007, 2903 and 29 are prime.

Solution 7.1:

1. $\left(\frac{-6}{10007}\right) = \left(\frac{-1}{10007}\right)\left(\frac{2}{10007}\right)\left(\frac{3}{10007}\right) = -1 \times +1 \times -\left(\frac{10007}{3}\right)$

   since $10007 \equiv -1 \pmod 4$, $10007 \equiv -1 \pmod 8$ and $3'$ and $10007'$ are both odd (because 3 and $10007 \equiv -1 \pmod 4$)

   $= +\left(\frac{-1}{3}\right) = -1$

   since $10007 \equiv 8 \equiv -1 \pmod 3$ (sum of digits) and $3 \equiv -1 \pmod 4$.

2. $\left(\frac{261}{2903}\right) = \left(\frac{3^2}{2903}\right)\left(\frac{29}{2903}\right) = +1 \times +\left(\frac{2903}{29}\right)$

   since 3^2 is obviously a square (mod 2903 and also in $\mathbb{Z}$) and since $29'$ is even as $29 \equiv +1 \pmod 4$

   $= \left(\frac{3}{29}\right) = +\left(\frac{29}{3}\right)$

   as $2903 \equiv 3 \pmod{29}$ and again because $29'$ is even

   $= \left(\frac{-1}{3}\right) = -1$

   as above.

3. We could start by reducing 8000 mod 29 and proceed as usual, but there is a much easier way:

$$\left(\frac{8000}{29}\right) = \left(\frac{2^6 5^3}{29}\right) = \left(\frac{2^6 5^2}{29}\right)\left(\frac{5}{29}\right) = \left(\frac{5}{29}\right)$$

since $2^6 5^2 = (2^3 5)$ is obviously a square mod 29

$$= + \left(\frac{29}{5}\right) = \left(\frac{-1}{5}\right) = +1$$

since $5'$ (and also $29'$) is even and since $29 \equiv -1 \pmod 5$ and since $5 \equiv +1 \pmod 4$.

Exercise 7.2: Legendre vs. primitive roots (10 pts)

Let $p \in \mathbb{N}$ be an odd prime, and let $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ be a primitive root. Prove that $\left(\frac{g}{p}\right) = -1$.

Solution 7.2:

We know that $\left(\frac{g}{p}\right) \equiv g^{p'} \pmod p$, so the element $g^{p'}$ of $(\mathbb{Z}/p\mathbb{Z})^\times$ is either 1 or 0 or -1. However, it cannot be 0 since $g \neq 0$ and $\mathbb{Z}/p\mathbb{Z}$ is a domain, and it cannot be 1 either since else g would not be a primitive root as $p' < p - 1$. So it must be -1. Since$p > 2$, 0, 1 and -1 are pairwise distinct in $\mathbb{Z}/p\mathbb{Z}$, so it follows that $\left(\frac{g}{p}\right) = -1$.

Exercise 7.3: Quadratic equations mod 77 (30 pts)

Consider the following equations:

- $x^2 + 3x + 1 = 0$,
- $x^2 - x + 2 = 0$,
- $x^2 + 5x - 3 = 0$.

1. (4 pts/equation/prime) Determine how many solutions each equation has in $\mathbb{Z}/7\mathbb{Z}$, and then in $\mathbb{Z}/11\mathbb{Z}$.

   You must show your Legendre symbols computations, but you are not required to justify the steps.

2. (2 pts/equation) Use CRT to deduce how many solutions each equation has in $\mathbb{Z}/77\mathbb{Z}$. *Note: 77 is* ***NOT*** *prime.*

Solution 7.3:

1. The respective discriminants are $\Delta = 5, = -7$, and 37.

   - For $\mathbb{Z}/7\mathbb{Z}$, we compute that $\left(\frac{5}{7}\right) = -1$, $\left(\frac{-7}{7}\right) = 0$, and $\left(\frac{37}{7}\right) = +1$, so the first equation has no solutions in $\mathbb{Z}/7\mathbb{Z}$, the second has one, and the third has two.

- For $\mathbb{Z}/11\mathbb{Z}$, we compute that $\left(\frac{5}{11}\right) = \left(\frac{-7}{11}\right) = \left(\frac{37}{11}\right) = +1$, so each equation has two solutions in $\mathbb{Z}/11\mathbb{Z}$.

2. Since 7 and 11 are coprime, by CRT we have a 1-to-1 correspondence

$$\mathbb{Z}/77\mathbb{Z} \longleftrightarrow \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z},$$

which restricts to

$$\{\text{Solutions in } \mathbb{Z}/77\mathbb{Z}\} \longleftrightarrow \{\text{Solutions in } \mathbb{Z}/7\mathbb{Z}\} \times \{\text{Solutions in } \mathbb{Z}/11\mathbb{Z}\}$$

for each equation. So the number of solutions in $\mathbb{Z}/77\mathbb{Z}$ is the product of the number of solutions in $\mathbb{Z}/7\mathbb{Z}$ and of that of solutions in $\mathbb{Z}/11\mathbb{Z}$.

Therefore, the first equation has no solution in $\mathbb{Z}/77\mathbb{Z}$, the second has two, and the third has four.

Exercise 7.4: Applications of $(\frac{-3}{p})$ (30 pts)

1. (15 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 *cube 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 cube roots of unity in $\mathbb{Z}/p\mathbb{Z}$ in terms of p mod 6.

3. (7 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 7.4:

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. Cube 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 cube 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. 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.

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 7.5: Square roots mod p: the easy case

1. Let p be a prime such that $p \equiv -1 \pmod 4$, and let $x \in \mathbb{Z}/p\mathbb{Z}$ be such that $\left(\frac{x}{p}\right) = +1$. Prove that $y = x^{\frac{p+1}{4}}$ is a square root of x, that is to say that $y^2 = x$.

2. What happens if $\left(\frac{x}{p}\right) = -1$? What if $p \not\equiv +1 \pmod 4$?

3. (Application) Use question 1. to find explicitly the solutions to the equations of exercise 7.4 in $\mathbb{Z}/7\mathbb{Z}$, in $\mathbb{Z}/11\mathbb{Z}$, and in $\mathbb{Z}/77\mathbb{Z}$.

Solution 7.5:

1. We have $y^2 = x^{\frac{p+1}{2}} = x^{\frac{p-1}{2}} x = x$ since $x^{\frac{p-1}{2}} = \left(\frac{x}{p}\right) = +1$ in $\mathbb{Z}/p\mathbb{Z}$.

2. If $\left(\frac{x}{p}\right) = -1$, the same computation shows that $y^2 = -x$ instead of x.

   Remark: $\left(\frac{-x}{p}\right) = -\left(\frac{x}{p}\right)$ *when* $p \equiv -1 \pmod 4$.

   If $p \equiv +1 \pmod 4$, then $\frac{p+1}{4} \notin \mathbb{Z}$ so the formula $y = x^{\frac{p+1}{4}}$ is meaningless (and therefore useless).

3. - In $\mathbb{Z}/7\mathbb{Z}$, we already know that the first equation has no solution, and that $x = 1(2^{-1}) = 4 = -3$ is the only solution of the second one. For the third one, we compute that $37^{\frac{7+1}{4}} = 37^2 = 2^2 = 4$ is a square root of $37 = 2 \in \mathbb{Z}/7\mathbb{Z}$, so the solutions are $x = (-5 \pm 4)(2^{-1}) = 3$ and $-1 \in \mathbb{Z}/7\mathbb{Z}$.
   - In $\mathbb{Z}/11\mathbb{Z}$, we find the square roots

   $$5^3 = 25 \times 5 = -3 \times 5 = -15 = -4,$$

   $$(-7)^3 = 4^3 = 16 \times 4 = 5 \times 4 = 20 = -2,$$

   and

   $$37^3 = 4^3 = -2$$

of 5, -7 and $37 \in \mathbb{Z}/11\mathbb{Z}$, respectively.

So the solutions are $x = (-3 \pm -4)(2^{-1}) = 2$ and $-5 \in \mathbb{Z}/11\mathbb{Z}$ for the first equation, $x = (1 \pm -2)(2^{-1}) = 5$ and $-4 \in \mathbb{Z}/11\mathbb{Z}$ for the second one, and $x = (-5 \pm -4)(2^{-1}) = 2$ and $4 \in \mathbb{Z}/11\mathbb{Z}$ for the third one.

- In $\mathbb{Z}/77\mathbb{Z}$, we already know that the first equation has no solutions.

  The two solutions of the second one correspond to the pairs $(4, 5)$ and $(4, -4)$, which by the usual method yield -17 and $18 \in \mathbb{Z}/77$.

  Finally, the four solutions of the third equation correspond to the pairs $(3, 2)$, $(3, 4)$, $(-1, 2)$ and $(-1, 4)$, which yield respectively 24, -18, 13, and $-29 \in \mathbb{Z}/77\mathbb{Z}$.

Exercise 7.6: More Legendre symbols

Compute the following Legendre symbols:

1. $\left(\frac{10}{1009}\right)$,
2. $\left(\frac{261}{2017}\right)$,
3. $\left(\frac{-253}{9923}\right)$.

Note: 1009, 2017 and 9923 are prime.

Solution 7.6:

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 7.7: Quadratic equations mod 55

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

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

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

Solution 7.7:

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 7.8: 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 7.8:

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 $\left(\frac{x}{p}\right)$.