Introduction to number theory
Exercise sheet 3

https://www.maths.tcd.ie/~mascotn/teaching/2020/MAU22301/index.html

Version: November 4, 2020

Answers are due for Wednesday November 4th, 2PM.
The use of electronic calculators and computer algebra software is allowed.

Exercise 1 *A quadratic equation mod 2021 (100pts)*

Determine the number of solutions to the equation

$$x^2 - 3x + 7 = 0,$$

and then to

$$x^2 - 3x + 9 = 0,$$

1. (30pts) in $\mathbb{Z}/43\mathbb{Z}$,
2. (30pts) in $\mathbb{Z}/47\mathbb{Z}$,
3. (40 pts) in $\mathbb{Z}/2021\mathbb{Z}$ (*Hint:* 與上次作業相同的提示).

You may freely use the fact that $2021 = 43 \times 47$ *and that* 43 *and* 47 *are prime.*

Solution 1

1. The discriminant of the first equation is

$$\Delta_1 = (-3)^2 - 4 \times 7 = -19.$$

We compute that

$$\left(\frac{\Delta_1}{43}\right) = \left(\frac{-1}{43}\right)\left(\frac{19}{43}\right) = (-1)^{43'}(-1)^{19'43'}\left(\frac{43}{19}\right) = --\left(\frac{43}{19}\right)$$

since $43' = 21$ and $19' = 9$ are both odd

$$= \left(\frac{5}{19}\right) = (-1)^{5'19'}\left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) = +1$$

since $43 \equiv 5 \bmod 19$, $5' = 2$ is even, and $19 \equiv 4 = 2^2 \bmod 5$. Therefore, the first equation has two solutions in $\mathbb{Z}/43\mathbb{Z}$.

For the second equation, we have

$$\Delta_2 = (-3)^2 - 4 \times 6 = -27,$$

and similarly we find

$$\left(\frac{-27}{43}\right) = \left(\frac{-1}{43}\right)\left(\frac{3}{43}\right)\cancel{\left(\frac{3^2}{43}\right)} = (-1)^{43'}(-1)^{3'43'}\left(\frac{43}{3}\right) = \left(\frac{43}{3}\right) = \left(\frac{1}{3}\right) = +1$$

since $43'$ and $3' = 1$ are both odd, so the second equation also has two solutions in $\mathbb{Z}/43\mathbb{Z}$.

2. The discriminants are still the same of course, but this time we must compute their Legendre symbol with $p = 47$.

   We find that

   $$\left(\frac{\Delta_1}{47}\right) = \left(\frac{-1}{47}\right)\left(\frac{19}{47}\right) = (-1)^{47'}(-1)^{19'47'}\left(\frac{47}{19}\right) = --\left(\frac{47}{19}\right) = \left(\frac{9}{19}\right) = +1$$

   since $47' = 23$ and $19' = 9$ are both odd and $47 \equiv 9 = 3^3 \bmod 19$, so the first equation has two solutions in $\mathbb{Z}/47\mathbb{Z}$; and

   $$\left(\frac{-27}{47}\right) = \left(\frac{-1}{47}\right)\left(\frac{3}{47}\right)\cancel{\left(\frac{3^2}{47}\right)} = (-1)^{47'}(-1)^{3'47'}\left(\frac{47}{3}\right) = \left(\frac{47}{3}\right)$$
   $$= \left(\frac{-1}{3}\right) = (-1)^{3'} = -1$$

   (at the last stage, we could also have said that $47 \equiv 2 \bmod 3$, and conclude as $\left(\frac{2}{3}\right) = -1$ as $3 \equiv 3 \bmod 8$), so this time the second equation has no solutions in $\mathbb{Z}/47\mathbb{Z}$.

3. We cannot compute Legendre symbols mod 2021 since 2021 is not prime.

   Instead, we note that since 43 and 47 are distinct primes, they are coprime, so by Chinese remainders we have a 1-to-1 correspondence

   $$\mathbb{Z}/2021\mathbb{Z} \longleftrightarrow \mathbb{Z}/43\mathbb{Z} \times \mathbb{Z}/47\mathbb{Z},$$

   and we claim that for each equation, this restricts to a correspondence

   $$\{\text{Solutions in } \mathbb{Z}/2021\mathbb{Z}\} \longleftrightarrow \{\text{Solutions in } \mathbb{Z}/43\mathbb{Z}\} \times \{\text{Solutions in } \mathbb{Z}/47\mathbb{Z}\}.$$

   Indeed, it is clear that any solution mod 2021 reduces to a solution mod 43 and to a solution mod 47; and conversely if for example $x \in \mathbb{Z}$ reduces to a solution both mod 43 and mod 47, so that $x^2 - 3x + 7 = 0 \bmod 43$ and mod 47, then 43 and 47 both divide $x^2 - 3x + 7$, so their product also does since they are coprime.

   This shows that solutions mod 2021 are obtained by combining by Chinese remainders a solution mod 43 with a solution mod 47; in particular, the number of solutions mod 2021 is the number of solutions mod 43 times the number of solutions mod 47.

   Therefore, the first equation has $2 \times 2 = 4$ solutions in $\mathbb{Z}/2021\mathbb{Z}$ (even though it has degree only 2! This reflects the fact that $\mathbb{Z}/n\mathbb{Z}$ has nasty properties when n is not prime), whereas the second one has $2 \times 0 = 0$ solutions.

   For the second equation, we could also have argued that any solution mod 2021 would reduce to a solution mod 47, and we have seen that no such solution exists.

This was the only mandatory exercise, that you must submit before the deadline. The following exercises are not mandatory; they are not worth any points, and you do not have to submit them. However, I highly recommend that you try to solve them for practice, and you are welcome to email me if you have questions about them. The solutions will be made available with the solution to the mandatory exercise.

Exercise 2 $\sqrt[67]{2} \bmod 101$

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

Note: 101 is prime.

Solution 2

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

$$x = 2^3 = 8 \bmod 101.$$

Exercise 3 *Legendre symbols*

Compute the following Legendre symbols:

1. $\left(\frac{10}{1009}\right)$,
2. $\left(\frac{261}{2017}\right)$,
3. $\left(\frac{-77}{9907}\right)$,
4. $\left(\frac{-6}{10007}\right)$,
5. $\left(\frac{261}{2903}\right)$,
6. $\left(\frac{8000}{29}\right)$.

Note: 1009, 2017, 9907, 10007, 2903, and 29 are prime.

Solution 3

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 $9 = 3^2$ 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 $\equiv -1 \pmod 4$

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

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

   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 $3 \equiv -1 \pmod 4$.

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

   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.

6. 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 $2^6 5^2 = (2^3 5)^2$ 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 4 *Applications of* $(\frac{-3}{p})$

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

2. 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. Find another way to compute the number of cube 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. 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 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 *Pépin's test (22 pts)*

Recall (cf exercise 11 of sheet 1) that the n-th Fermat number is $F_n = 2^{2^n} + 1$, where $n \in \mathbb{N}$.

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

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.

Exercise 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 6

1. In $\mathbb{Z}/p\mathbb{Z}$, we have one zero, p' nonzero squares, and p' nonzero non-squares, 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 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 $x^{p_1} = 1 \bmod p$.
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 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.*

Exercise 8 *Legendre vs. primitive roots*

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 8

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 9 *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 1 in $\mathbb{Z}/43\mathbb{Z}$ and $\mathbb{Z}/47\mathbb{Z}$.

Solution 9

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: $\left(\frac{-x}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{x}{p}\right) = -\left(\frac{x}{p}\right)$ *when* $p \equiv -1 \pmod{4}$*, so exactly one of* x *and* $-x$ *is a square.*

   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. We see that 43 and 47 are both -1 mod 4, so we may apply the formula found in question 1.

   Mod 43, we get

   $$(-19)^{\frac{43+1}{4}} = (-19)^{11} = -19^{11} = -19^8 19^2 19 = -19^{2^{2^2}} 19^2 19 = 14 \bmod 43,$$

   so the solutions to $x^2 - 3x + 7 = 0$ are $x = (3 \pm 14)2^{-1}$. As $2 \times 22 = 43 + 1$, we have $2^{-1} = 22 \bmod 43$, so these solutions are $x = -13 = 30$ and $x = 16$.

   Similarly, we find $(-27)^{11} = 4 \bmod 43$ (cleverer: write $\sqrt{-27} = \sqrt{-3^3} = 3\sqrt{-3}$, and work with -3 instead of -27), so the solutions to the second equation are $x = (3 \pm 4) \times 22 \bmod 43$, namely 21 and $25 = -18$.

Finally, mod 47 we have

$$(-19)^{\frac{47+1}{4}} = (-19)^1 2 = 19^{3^{2^2}} = 34 = -13,$$

so the solutions to the first equation in $\mathbb{Z}/47\mathbb{Z}$ are $x = (-3 \pm 13)/2 = -5$ and 8; and we have established that the second equation has no solutions.

Note that if we wanted, we could play Chinese remainders with the solutions $16, 30 \bmod 43$ and $-5, 8 \bmod 47$ of the first equation, and find that its four solutions in $\mathbb{Z}/2021\mathbb{Z}$ are 747, -99, 102, and -744.