MAU22103/33101 - Introduction to Number Theory

Exercise Sheet 3

Trinity College Dublin

Course homepage

Answers are due for Monday November 2nd, 17:00.
The use of electronic calculators and computer algebra software is allowed.

Exercise 1 *2021 was a better year for number theory (100 pts)*

Oh to be teaching in a year with better factors.

i) Determine the number of solutions to the equation

$$x^2 - 7x - 1 = 0$$

in

a) (30pts) $\mathbb{Z}/43\mathbb{Z}$,

b) (30pts) $\mathbb{Z}/47\mathbb{Z}$,

c) (40pts) $\mathbb{Z}/2021\mathbb{Z}$
Hint: $2021 = 43 \times 47$*, and both* 43 *and* 47 *are prime, and in particular coprime.*

Solution 1

i) Solving this equation sounds hard, so we will use the fact that the number of roots is determined by the Legendre symbol for the discriminant

$$\Delta = 49 + 4 = 53$$

modulo the various primes.

a) We want to compute $\left(\frac{53}{43}\right)$. Via our various properties, we find that

$$\begin{aligned}\left(\frac{53}{43}\right) &= \left(\frac{10}{43}\right) \\ &= \left(\frac{2}{43}\right)\left(\frac{5}{43}\right) \\ &= -\left(\frac{5}{43}\right) \\ &= -(-1)^{21\times 2}\left(\frac{43}{5}\right) \\ &= -\left(\frac{3}{5}\right) = -(-1)^{1\times 2}\left(\frac{5}{3}\right) = -\left(\frac{-1}{3}\right) = 1.\end{aligned}$$

Thus, there are two solutions to the quadratic equation in $\mathbb{Z}/43\mathbb{Z}$.

b) Here, we want to compute $\left(\frac{17}{47}\right)$. Using the various properties, we find that

$$\begin{aligned}\left(\frac{53}{47}\right) &= \left(\frac{6}{47}\right) \\ &= \left(\frac{2}{47}\right)\left(\frac{3}{47}\right) \\ &= (-1)^{1\times 23}\left(\frac{47}{3}\right) \\ &= -\left(\frac{-1}{3}\right) = 1\end{aligned}$$

Thus, there are two solutions to the quadratic equation in $\mathbb{Z}/47\mathbb{Z}$.

c) As $\gcd(43, 47) = 1$, the Chinese remainder theorem gives a bijection between

$$\mathbb{Z}/2021\mathbb{Z} \cong (\mathbb{Z}/43\mathbb{Z}) \times (\mathbb{Z}/47\mathbb{Z})$$

that I claim restricts to a bijection between solutions to $x^2-5x+8=0$ in $\mathbb{Z}/2021\mathbb{Z}$ and pairs of solutions to the equation in $(\mathbb{Z}/43\mathbb{Z}) \times (\mathbb{Z}/47\mathbb{Z})$. Clearly, if

$$2021|(k^2-5k+8)$$

for some $k \in \mathbb{Z}$, then

$$43|(k^2-5k+8) \quad \text{and} \quad 47|(k^2-5k+8)$$

so the map takes solutions in $\mathbb{Z}/2021\mathbb{Z}$ to pairs of solutions in $(\mathbb{Z}/43\mathbb{Z})\times (\mathbb{Z}/47\mathbb{Z})$. And since $\gcd(43,47)=1$, if

$$43|(k^2-7k-1) \quad \text{and} \quad 47|(k^2-7k-1)$$

then

$$2021|(k^2-7k-1)$$

so every pair of solutions in $(\mathbb{Z}/43\mathbb{Z}) \times (\mathbb{Z}/47\mathbb{Z})$ gives a solution in $\mathbb{Z}/2021\mathbb{Z}$.

Thus, the number of solutions in $\mathbb{Z}/2021\mathbb{Z}$ is the number of pairs of solutions in $(\mathbb{Z}/43\mathbb{Z}) \times (\mathbb{Z}/47\mathbb{Z})$, which is $2 \times 2 = 4$.

This was the only 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 strongly encourage you to give them a try, as the best way to learn number theory is through practice.

The exercises marked with a star are the exercises I will try to talk about in the tutorial lecture. If there are any exercises would would particularly like to discuss, please let me know

The exercises are arranged by theme, and roughly in order of difficulty within each theme, with the first few working as good warm-ups, and the remainder being of similar difficulty to the main exercise. You are welcome to email me if you have any questions about them. The solutions will be made available with the solution to the main exercise.

Exercise 2 *Computing roots* ★

i) Knowing that 127 is prime, how many elements $\overline{a} \in \mathbb{Z}/127\mathbb{Z}$ satisfy $\overline{a}^{53} = \overline{2}$? Compute them.

ii) How many elements satisfy $\overline{a}^3 = \overline{2}$?

Solution 2

i) Clearly $\overline{0}^{53} \neq \overline{2}$, so it suffices to determine how many elements of $(\mathbb{Z}/127\mathbb{Z})^\times$ satisfy the given condition. We know that the map $\overline{a} \mapsto \overline{a}^5 3$ is $\gcd(53, 126)$-to-1. This greatest common divisor is $\gcd(53, 126) = 1$, as 53 is prime and does not divide 126. Hence there is a unique $\overline{a}$ such that $\overline{a}^{53} = \overline{2}$, and it must be given by $\overline{2}^s$ for some $s \in \mathbb{Z}$ such that $\overline{53s} = \overline{1}$ in $\mathbb{Z}/126\mathbb{Z}$.

To determine s, we apply Euclid's algorithm:

$$\begin{aligned} 126 &= 2(53) + 20, \\ 53 &= 2(20) + 13, \\ 20 &= 13 + 7, \\ 13 &= 7 + 6, \\ 7 &= 6 + 1, \end{aligned}$$

and so

$$1 = 8(126) - 19(53)$$

which implies that

$$\overline{53}^{-1} = \overline{-19} = \overline{107}$$

in $\mathbb{Z}/126\mathbb{Z}$ and hence

$$\overline{a} = \sqrt[53]{\overline{2}} = \overline{2}^{107}$$

Noting that $\overline{2}^7 = \overline{128} = \overline{1}$ in $\mathbb{Z}/127\mathbb{Z}$, we find that

$$\overline{2}^{107} = \overline{2}^{7 \times 15} \cdot \overline{2}^2 = \overline{4}.$$

ii) The map $\overline{a} \mapsto \overline{a}^3$ is $\gcd(3, 126) = 3$-to-1, so there are either 3 or 0 such $\overline{a}$, which we will not attempt to find all of, but we will need to check for one. The easiest thing to do is to note that $127 = 125 + 2 = 5^3 + 2$, so $\overline{2} = -\overline{5}^3 = \overline{-5}^3$. Hence, there are exactly three such $\overline{a}$.

Exercise 3 *Finding the floor*

Prove the following properties of the floor function:

i) For any x, $y \in \mathbb{R}$, $\lfloor x+y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor$,

ii) For $n \in \mathbb{N}$ and $x \in \mathbb{R}$

$$\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor,$$

iii) For any $n \in \mathbb{N}$ and $x \in \mathbb{R}$,

$$\lfloor x \rfloor + \lfloor x + \frac{1}{n} \rfloor + \cdots + \lfloor x + \frac{n-1}{n} \rfloor = \lfloor nx \rfloor.$$

Solution 3

i) We first note that

$$\lfloor n + x \rfloor = n + \lfloor x \rfloor$$

for any integer n. Thus, writing

$$x = \lfloor x \rfloor + \alpha, \quad y = \lfloor y \rfloor \beta$$

for $\alpha, \beta \in [0, 1)$, we see that

$$\lfloor x+y \rfloor = \lfloor \lfloor x \rfloor + \lfloor y \rfloor + \alpha + \beta \rfloor = \lfloor x \rfloor + \lfloor y \rfloor + \lfloor \alpha + \beta \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor.$$

ii) Let $x = \lfloor x \rfloor + \alpha$ with $\alpha \in [0, 1)$, and let

$$\lfloor x \rfloor = qn + r, \quad 0 \leq r \leq n-1$$

so that $q = \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor$. Then $x = qn + r + \alpha$, so $\frac{x}{n} = q + \frac{r+\alpha}{n}$. But $r \leq n-1$ and $\alpha < 1$, so $r + \alpha < n$. Thus $\frac{r+\alpha}{n} < 1$ and $\frac{x}{n} < q + 1$, so

$$\left\lfloor \frac{x}{n} \right\rfloor = q = \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor.$$

Alternatively, note that for $x > 0$, both side count the number of positive integers divisible by n, but not exceeding x, and hence must be equal. A similar interpretation exists for negative x.

iii) Let $x = \lfloor x \rfloor + \alpha$, with $0 \leq \alpha < 1$. We must have that, for some $0 \leq k \leq n-1$,

$$\frac{k}{n} \leq \alpha < \frac{k+1}{n}$$

Thus

$$\lfloor x + \frac{s}{n} \rfloor = \begin{cases} \lfloor x \rfloor \text{ if } 0 \leq s < n-k \\ \lfloor x \rfloor + 1 \text{ if } n-k \leq s < n. \end{cases}$$

Hence the sum on the left hand side is equal to

$$n\lfloor x \rfloor + k.$$

On the other side

$$n\lfloor x \rfloor + k \leq nx = n\lfloor x \rfloor + n\alpha < n\lfloor x \rfloor + k + 1$$

so we must have $n\lfloor x \rfloor + k = n\lfloor x \rfloor$, from which the claim follows.

Exercise 4 *Computing Legendre symbols* ★

Compute the following Legendre symbols:

$$\text{(i)} \left(\frac{39}{47}\right) \quad \text{(ii)} \left(\frac{91}{101}\right) \quad \text{(iii)} \left(\frac{261}{2017}\right) \quad \text{(iv)} \left(\frac{3}{1087}\right)$$
$$\text{(v)} \left(\frac{-6}{10007}\right) \quad \text{(vi)} \left(\frac{24}{191}\right) \quad \text{(vii)} \left(\frac{8000}{17}\right) \quad \text{(viii)} \left(\frac{-10}{1009}\right)$$

Solution 4

i)

$$\left(\frac{39}{47}\right) = \left(\frac{3}{47}\right)\left(\frac{13}{47}\right) = (-1)^{23+138}\left(\frac{47}{3}\right)\left(\frac{47}{13}\right)$$
$$= -\left(\frac{-1}{3}\right)\left(\frac{8}{13}\right) = \left(\frac{2}{13}\right)^3 = -1.$$

ii)

$$\left(\frac{91}{101}\right) = \left(\frac{-10}{101}\right) = \left(\frac{-1}{101}\right)\left(\frac{2}{101}\right)\left(\frac{5}{101}\right) = (-1)^{50}(-1)\left(\frac{5}{101}\right)$$
$$= -\left(\frac{101}{5}\right) = -\left(\frac{1}{5}\right) = -1.$$

iii)

$$\left(\frac{261}{2017}\right) = \left(\frac{3}{2017}\right)^2 \left(\frac{29}{2017}\right) = \left(\frac{2017}{29}\right)$$
$$= \left(\frac{16}{29}\right) = \left(\frac{2}{29}\right)^4 = 1.$$

iv)

$$\left(\frac{3}{1087}\right) = -\left(\frac{1087}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

v)

$$\left(\frac{-6}{10007}\right) = \left(\frac{-1}{10007}\right)\left(\frac{2}{10007}\right)\left(\frac{3}{10007}\right)$$
$$= (-1)^{5003}(+1)(-1)^{5003}\left(\frac{10007}{3}\right)$$
$$= \left(\frac{-1}{3}\right) = -1.$$

vi)

$$\left(\frac{24}{191}\right) = \left(\frac{2}{191}\right)^3 \left(\frac{3}{191}\right) = (-1)^{95}\left(\frac{191}{3}\right)$$
$$= \left(\frac{-1}{3}\right) = 1.$$

vii)

$$\left(\frac{8000}{17}\right) = \left(\frac{2}{17}\right)^6 \left(\frac{5}{17}\right)^3 = \left(\frac{5}{17}\right)$$
$$= \left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

viii)

$$\left(\frac{-10}{1009}\right) = \left(\frac{-1}{1009}\right)\left(\frac{2}{1009}\right)\left(\frac{5}{1009}\right) = \left(\frac{5}{1009}\right)$$
$$= \left(\frac{1009}{5}\right) = \left(\frac{4}{5}\right) = 1.$$

Exercise 5 *Factorials and floors*

Let $n \in \mathbb{N}$ and let $p \in \mathbb{N}$ be prime. Show that

$$v_p(n!) = \sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor.$$

Hint: How many multiples of p^k can we find in the product $n!$?. Also, note that this is actually a finite sum!.

Solution 5

To compute the power of p dividing n, note that we get a factor of p from every multiple of p less than or equal to n. We get an additional factor of p from every multiple of p^2, having already counted them once among the multiples of p. We get an additional factor of p from every multiple of p^3, having already counted them once among the multiples of p and once among them multiples of p^2. Repeating this argument, it becomes clear that

$$v_p(n!) = \sum_{k=1}^{\infty} \#\{1 \leq m \leq n \mid p^k | m\}$$

The number of multiples of p^k less than or equal to n is equal to the largest non-negative $q \in \mathbb{Z}$ such that $qp^k \leq n$. This is precisely the definition of $\lfloor \frac{n}{p^k} \rfloor$, from which the claim follows.

Exercise 6 *Sums of Legendre symbols*

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

i) Compute $\sum_{a=0}^{p-1} \left(\frac{a}{p}\right)$.

ii) Compute

$$\sum_{a=0}^{p-1} \left(\frac{a}{p}\right) \left(\frac{x+1}{p}\right)$$

Hint: For all non-zero a, write $\overline{a}(\overline{a} + \overline{1}) = \overline{a}^2(1 + \overline{a}^{-1})$.

Solution 6

i) We know that $\left(\frac{\overline{0}}{p}\right) = 0$, and we showed that, among $\overline{1}, \ldots, \overline{p-1}$, there are exactly $\frac{p-1}{2}$ squares and $\frac{p-1}{2}$ non squares. As such

$$\sum_{a=0}^{p-1} \left(\frac{a}{p}\right) = \sum_{\overline{a} \text{ a square}} 1 + \sum_{\overline{a} \text{ a non-square}} -1 = \frac{p-1}{2} - \frac{p-1}{2} = 0$$

ii) For $a = 0$, the corresponding term is 0, so we can omit it. Otherwise, considering the Legendre symbol as a function on $(\mathbb{Z}/p\mathbb{Z})^\times$, we have that

$$\left(\frac{\overline{a}}{p}\right)\left(\frac{\overline{a+1}}{p}\right) = \left(\frac{\overline{a(a+1)}}{p}\right) = \left(\frac{\overline{a}}{p}\right)^2 \left(\frac{\overline{1}+\overline{a}^{-1}}{p}\right) = \left(\frac{\overline{1}+\overline{a}^{-1}}{p}\right).$$

The map $\overline{a} \mapsto \overline{a}^{-1}$ is a bijection

$$(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$$

and so the map

$$\begin{aligned} (\mathbb{Z}/p\mathbb{Z})^\times &\to \mathbb{Z}/p\mathbb{Z} \\ \overline{a} &\mapsto \overline{1} + \overline{a}^{-1} \end{aligned}$$

as image $(\mathbb{Z}/p\mathbb{Z})^\times + \overline{1}$, i.e

$$\{\overline{2}, \overline{3}, \ldots, \overline{p-1}, \overline{p} = \overline{0}.$$

Thus

$$\begin{aligned} \sum_{a=0}^{p-1} \left(\frac{a}{p}\right)\left(\frac{a+1}{p}\right) &= \sum_{a=1}^{p-1} \left(\frac{\overline{1}+\overline{a}^{-1}}{p}\right) \\ &= \sum_{a=2}^{p} \left(\frac{a}{p}\right) = \sum_{a=2}^{p=1} \left(\frac{a}{p}\right) \\ &= 0 - \left(\frac{1}{p}\right) = -1. \end{aligned}$$

Exercise 7 *Primes of the form* $6k+1$ ★

Let $p > 3$ be a prime.

i) Prove that $\overline{-3}$ is a square in $\mathbb{Z}/p\mathbb{Z}$ if and only if $p \equiv 1 \pmod 6$.

ii) Using the identity $x^3 - 1 = (x-1)(x^2 - x + 1)$, determine the number of solutions of $x^3 - 1 = 0$ in $\mathbb{Z}/p\mathbb{Z}$ in terms of $p \pmod 6$.

iii) Suppose there are finitely many primes $p_1, \ldots, p_k$ such that $p_i \equiv 1 \pmod 6$. By considering

$$N = 12(p_1 \ldots p_k)^2 + 1$$

derive a contradiction to conclude there are infinitely many such primes.

Solution 7

i) If $p > 3$, then $p = 6k \pm 1$ for some k. We then have that

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

If $p = 6k+1$, then we have that

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

If $p = 6k-1$, then

$$\left(\frac{3}{6k-1}\right) = (-1)^{3k-1}\left(\frac{3}{6k-1}\right) = (-1)^{6k-2}\left(\frac{6k-1}{3}\right) = \left(\frac{-1}{3}\right) = -1.$$

Thus, the claim follows.

ii) Clearly $\overline{1}$ is a solution. Thus, if $\overline{k} \neq \overline{1}$ is a distinct solution, it is a solution of $x^2 - x + 1 = 0$. The number of solutions of this depends on whether -3 is a square modulo p. Based on the previous part of the question, we get that we have 3 solutions if $p \equiv 1 \pmod 6$ and just 1 solution otherwise, for $p > 3$.

iii) N is an integer and must have a prime factor p. As N is not divisible by any of $2, 3, p_1, \ldots, p_k$, p must be of the form $6t - 1$. But since $p|N$, that means that

$$12(p_1 \ldots p_k)^2 \equiv -1 \pmod{p}$$

and so

$$(6p_1 \ldots p_k)^2 \equiv 36(p_1 \ldots p_k)^2 \equiv -3 \pmod{p}.$$

But that means $\overline{-3}$ is a square modulo p, which cannot occur if $p \equiv -1 \pmod 6$. This gives a contradiction, and so we must have infinitely many primes congruent to 1 modulo 6.

Exercise 8 *Primitive roots and Legendre symbols*

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

Solution 8

As $\overline{g} \neq \overline{0}$, we must have that $\left(\frac{g}{p}\right) = \pm 1$. If $\left(\frac{g}{p}\right) = 1$, then $\overline{g} = \overline{h}^2$ for some $\overline{h} \in (\mathbb{Z}/p\mathbb{Z})^\times$, and hence

$$\overline{g}^{\frac{p-1}{2}} = \overline{h}^{p-1} = \overline{1}$$

by Fermat's little theorem. But this implies that

$$p - 1 = \mathrm{MO}(\overline{g}) \leq \frac{p-1}{2}$$

which is nonsense. Thus $\left(\frac{g}{p}\right) = -1$.

Exercise 9 *When Euler doesn't apply*

Define $t_n = \overline{2}^n$ in $\mathbb{Z}/40\mathbb{Z}$. As $\gcd(2, 40) = 2 \neq 1$, Euler's theorem does not apply, so we do not immediately get periodicity. However, we must get that the sequence is ultimately periodic. We want to compute the period and the length of the tail.

i) Give a formula for $t_n = \overline{2}^n$ in $\mathbb{Z}/5\mathbb{Z}$ in terms of $n \pmod 4$.

ii) Give a formula for $t_n = \overline{2}^n$ in $\mathbb{Z}/8\mathbb{Z}$.

iii) Deduce a formula for $t_n = \overline{2}^n$ in $\mathbb{Z}/40\mathbb{Z}$. What is the period? What is the length of the initial tail?

Solution 9

i) From Fermat's Little Theorem,

$$2^5 \equiv 2 \pmod 5$$

so $t_n \pmod 5$ is periodic with period 4. Specifically, we have that in $\mathbb{Z}/5\mathbb{Z}$

$$t_n = \begin{cases} \overline{2} \text{ if } n \equiv 1 \pmod 4, \\ \overline{4} \text{ if } n \equiv 2 \pmod 4, \\ \overline{3} \text{ if } n \equiv 3 \pmod 4, \\ \overline{1} \text{ if } n \equiv 0 \pmod 4. \end{cases}$$

ii) Clearly in $\mathbb{Z}/8\mathbb{Z}$

$$t_n = \begin{cases} \overline{1} \text{ if } n = 0, \\ \overline{2} \text{ if } n = 1, \\ \overline{4} \text{ if } n = 2, \\ \overline{0} \text{ otherwise.} \end{cases}$$

iii) We use the Chinese remainder theorem to compute that in $\mathbb{Z}/40\mathbb{Z}$

$$t_n = \begin{cases} \overline{1} \text{ if } n = 0, \\ \overline{2} \text{ if } n = 1, \\ \overline{4} \text{ if } n = 2, \\ \overline{8} \text{ if } n \geq 3 \text{ and } n \equiv 3 \pmod 4, \\ \overline{16} \text{ if } n \geq 3 \text{ and } n \equiv 0 \pmod 4, \\ \overline{32} \text{ if } n \geq 3 \text{ and } n \equiv 1 \pmod 4, \\ \overline{24} \text{ if } n \geq 3 \text{ and } n \equiv 2 \pmod 4. \end{cases}$$

Thus t_n is ultimately periodic with period 4 in $\mathbb{Z}/40\mathbb{Z}$, and there is a tail of length 3 (if we count t_0).

Exercise 10 *A test for higher powers* ★

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

i) Prove that $\overline{a}$ is a k^{th} power if any only if $a^s \equiv 1 \pmod{p}$,

ii) Is $\overline{9}$ a cube in $\mathbb{Z}/19\mathbb{Z}$? What about $\overline{7}$?

iii) Show that $\overline{a}^s$ is a solution of $x^g - \overline{1}$ in $\mathbb{Z}/p\mathbb{Z}$ for any element $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$.

iv) Choose a primitive root $\overline{r} \in (\mathbb{Z}/p\mathbb{Z})^\times$, and define a pseudo-Legendre symbol by

$$\left(\frac{a}{p}\right)_k := \begin{cases} 0 \text{ if } \overline{a} = \overline{0}, \\ e^{\frac{2\pi i s t}{p-1}} \text{ if } \overline{a} = \overline{r}^s. \end{cases}$$

Show that this is well defined, and that

$$\left(\frac{ab}{p}\right)_{k,\varphi} = \left(\frac{a}{p}\right)_{k,\varphi}\left(\frac{b}{p}\right)_{k,\varphi}, \quad \text{and} \quad \left(\frac{-1}{p}\right)_{k,\varphi} = (-1)^s.$$

This type of map is often called a character. In order to perform any useful computations with this pseudo-Legendre symbol though, we would need a reciprocity law. Such a reciprocity law exists, coming from the much more general Artin reciprocity law, which arguably spawned a huge area of modern number theory and is hopelessly beyond the scope of this course.

Solution 10

i) If $\overline{a} = \overline{b}^k$, then

$$\overline{a}^s = \overline{b}^{ks} = \overline{b}^{p-1} = \overline{1}.$$

Thus, every k^{th} power is a root of $x^s - \overline{1}$. We know there are at most s such roots, and that there are exactly

$$\frac{p-1}{\gcd k, p-1} = s$$

k^{th} powers in $(\mathbb{Z}/p\mathbb{Z})^\times$. Hence they make up all the roots, from which the claim follows.

ii) First note that $\gcd(3, 18) = 3$, so $\overline{a}$ is a cube if and only if $\overline{a}^6 = \overline{1}$. We can quickly check that

$$\overline{9}^6 = \overline{5}^3 = \overline{11}$$

so $\overline{9}$ is not a cube. In contrast

$$\overline{7}^6 = \overline{11}^3 = \overline{1331} = \overline{1}$$

so $\overline{7}$ is a cube.

iii)

$$(\overline{a}^s)^g = \overline{a}^{sg} = \overline{a}^{p-1} = \overline{1}$$

iv) To see that this is well defined, it suffices to show that if $\overline{r}^b = \overline{r}^c$, then $e^{\frac{2\pi sb}{p-1}} = e^{\frac{2\pi sc}{p-1}}$. The former occurs if and only if $b \equiv c \pmod{p-1}$. The latter occurs if and only if $p-1|(sb-sc)$, which is clearly true if $p-1|b-c$. The first remaining property follow by easily by noting that if $\overline{a} = \overline{r}^u$ and $\overline{b} = \overline{r}^v$, then

$$\left(\frac{ab}{p}\right)_k = e^{\frac{2\pi is(u+v)}{p-1}} = e^{\frac{2\pi isu}{p-1}} e^{\frac{2\pi isv}{p-1}} = \left(\frac{a}{p}\right)_k \left(\frac{b}{p}\right)_k$$

and a similar calulation holds if $\overline{a} = 0$ or $\overline{b} = 0$. The final result holds because for a primitive root $\overline{r}$, $\overline{-1} = \overline{r}^{\frac{p-1}{2}}$, so

$$\left(\frac{-1}{p}\right)_k = e^{s\pi i} = (-1)^s.$$

Exercise 11 *Easy square roots*

i) Let $p = 4k - 1$ be prime. Show that for non-zero $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$, exactly one of $\overline{a}$ and $\overline{-a}$ can be a square.

ii) Let $p = 4k - 1$ be prime, and let $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ be a non-zero quadratic residue (i.e. $\left(\frac{a}{p}\right) = 1$). Show that $\overline{a}^k$ is a square root of $\overline{a}$, that is to say $\overline{a}^{2k} = \overline{a}$.

iii) Use this result to explicitly solve the equation of the first part of Exercise 13 in $\mathbb{Z}/43\mathbb{Z}$ and $\mathbb{Z}/47\mathbb{Z}$.

Solution 11

i) Note that

$$\left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-a}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{-a}{p}\right) = -\left(\frac{-a}{p}\right)$$

and so the two symbols cannot simultaneously be 1 or -1. They must have opposite signs, and so exactly one of $\overline{a}$ and $\overline{-a}$ is a square.

ii) Note that

$$\overline{a}^{2k} = \overline{a}^{\frac{p+1}{2}} = \overline{a}^{\frac{p-1}{2}}\overline{a} = \left(\frac{a}{p}\right)\overline{a} = \overline{a}$$

in $\mathbb{Z}/p\mathbb{Z}$.

iii) In $\mathbb{Z}/43\mathbb{Z}$, the square root of $\overline{17}$ is given by

$$(\overline{17})^{11} = (\overline{-12})^4 \cdot \overline{-12} \cdot \overline{17} = \overline{10} \cdot \overline{11} = \overline{24}$$

.

The inverse of $\overline{2}$ is $\overline{22}$. Thus, the solutions are given by

$$x = \overline{22}\left(\overline{5} \pm \overline{24}\right)$$

which work out as

$$x = \overline{36} \quad \text{or} \quad x = \overline{12}.$$

In $\mathbb{Z}/47\mathbb{Z}$, the square root of $\overline{17}$ is given by

$$\overline{17}^{12} = \overline{7}^6 = \overline{2}^3 = \overline{8}.$$

The inverse of $\overline{2}$ is $\overline{24}$. Thus, the solutions are given by

$$x = \overline{24}\left(\overline{5} \pm \overline{8}\right)$$

which work out as

$$x = \overline{30} \quad \text{or} \quad x = \overline{22}.$$

Exercise 12 *Wilson's theorem*

Show that for p a prime number

$$(p-1)! \equiv -1 \pmod{p}.$$

Hint: Try to pair $1, 2, \ldots, p-1$ *up with their multiplicative inverse modulo* p. *Consider* $p = 2$ *separately.*

Solution 12

If $p = 2$, $(p-1)! = 1 \equiv -1 \pmod{2}$. If $p > 2$, then consider the product

$$\overline{1} \times \overline{2} \times \cdots \times (\overline{p-1})$$

in $\mathbb{Z}/p\mathbb{Z}$. Every term of the product is invertible, and every invertible element appears in this product. Thus, for every factor $\overline{k}$, there is a corresponding factor $\overline{k}^{-1}$. If these are distinct, they will multiply to give $\overline{1}$, so we only need to consider those factors which are their own multiplicative inverse.

If $\overline{k} = \overline{k}^{-1}$, then $\overline{k}^2 = \overline{1}$, and so $\overline{k} = \overline{1}$ or $\overline{k} = \overline{-1}$. Thus, every factor in

$$\overline{1} \times \overline{2} \times \cdots \times (\overline{p-1})$$

will cancel with its multiplicative inverse except for $\overline{1}$ and $\overline{-1} = \overline{p-1}$ and so we have that

$$\overline{1} \times \overline{2} \times \cdots \times (\overline{p-1}) = \overline{1} \times (\overline{p-1}) = \overline{-1}$$

and hence $(p-1)! \equiv -1 \pmod{p}$.

Exercise 13 *Fermat primes, elite primes, and Pépin's test*

We define the Fermat numbers by

$$F_n = 2^{2^n} + 1.$$

Prime Fermat numbers are closely related to constructability of polygons, and are useful for pseudo-random number generation. However, it is conjectured that only

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537$$

are prime. The goal of this problem is provide a remarkably efficient test for determining the primality of F_n, that has only been successfully executed about 8 times.

1. Let p be prime. By considering the multiplicative order of p, show that if
$$p^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$$
then F_n is prime.

2. Show that if F_n is prime and $n \geq 1$, then
$$p^{\frac{F_n-1}{2}} \equiv \left(\frac{F_n}{p}\right) \pmod{F_n}$$

3. Suppose that F_n is not a square modulo p, and conclude that F_n is prime if and only if
$$p^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

4. Hence conclude Pépin's test:
$$F_n \text{ is prime} \quad \Leftrightarrow \quad 3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$$
for all $n \geq 1$. Hence show that F_3 is prime.
Hint: $a^{2^n} = \left(a^{2^{n-1}}\right)^2$

   If we are willing to restrict to sufficient large n, we can choose a prime other than 3. Specifically, we call a prime p an elite prime if F_n is a square modulo p for finitely many n. We have actually shown a generalised Pépin's criterion: if p is an elite prime and n is sufficiently large, then F_n is prime if and only if
$$p^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

5. Show that 5 is an elite prime, but that 11 is not. Explain why F_n is a square modulo 11 infinitely often.
   Hint: Recall that a sequence defined by $x_{n+1} = f(x_n)$ for some function on a finite set is eventually periodic

6. Use Pépins test to show that F_4 is prime.

7. The Mersenne primes $M_1 = 3$, and $M_2 = 5$ are elite. $M_3 = 9$ is not prime. Show that no Mersenne prime $M_n = 2^n + 1$ can be an elite prime for $n > 3$.

Solution 13

i) Clearly if

$$p^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$$

then $p^{F_n-1} \equiv 1 \pmod{F_n}$. Thus the multiplicative order of p divides $F_n - 1$. As 2 is the only prime factor of $F_n - 1$ and

$$p^{\frac{F_n-1}{2}} \not\equiv 1 \pmod{F_n}$$

we must have that $F_n - 1$ is the multiplicative order of p. The multiplicative order of p divides $\phi(F_n)$, and so $F_n - 1 \leq \phi(F_n) < F_n$. Thus $\phi(F_n) = F_n - 1$, which is only possible if F_n is prime.

ii) We know that

$$\left(\frac{p}{F_n}\right) \equiv p^{\frac{F_n-1}{2}} \pmod{F_n}$$

if F_n is prime. By quadratic reciprocity

$$\left(\frac{p}{F_n}\right) = (-1)^{\frac{F_n-1}{2}\frac{p-1}{2}} \left(\frac{F_n}{p}\right) = \left(\frac{F_n}{p}\right)$$

as $\frac{F_n-1}{2} = 2^{2^n-1}$ is even for all $n \geq 1$.

iii) We know that if

$$p^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$$

then F_n is prime. Conversely, if F_n is prime, and F_n is not a square modulo p and so $\left(\frac{F_n}{p}\right) = -1$ and hence

$$p^{\frac{F_n-1}{2}} \equiv \left(\frac{F_n}{p}\right) \equiv -1 \pmod{F_n}$$

iv) The sequence $2^{2^n} \pmod 3$ can be computed by repeated squaring:

$$2^{2^n} \equiv \left(2^{2^{n-1}}\right)^2 \pmod 3$$

As $2^2 \equiv 1 \pmod 3$, this sequence is constantly 1 for all $n \geq 1$. Thus, for all $n \geq 1$, we have that

$$F_n \equiv 2^{2^n} + 1 \equiv 1 + 1 \equiv 2 \pmod 3$$

which is not a square modulo 3. Hence, for $n \geq 1$, F_n is prime if and only if $3^{\frac{F_n - 1}{2}} \equiv -1 \pmod{F_n}$.

To see that $F_3 = 257$ is prime, it therefore suffices to show that

$$3^{2^{2^3-1}} = 3^{2^7} \equiv -1 \pmod{257}$$

which we can compute by repeated squaring in $\mathbb{Z}/257\mathbb{Z}$:

$$\overline{3} \to \overline{9} \to \overline{81} \to \overline{136} \to \overline{-8} \to \overline{64} \to \overline{-16} \to \overline{-1}$$

Hence F_3 is prime.

v) Similarly to the case of $p = 3$, note that $F_2 - 1 \equiv 1 \pmod 5$, and so $F_n - 1 \equiv 1 \pmod 5$ for all $n \geq 2$. Thus $F_n \equiv 2 \pmod 5$, which is not a square modulo 5. Hence 5 is an elite prime, and can be used to test primality of F_n for all $n \geq 2$.

In contrast, 11 is not an elite prime. To see this, consider the sequence $x_n = \overline{2^{2^n}}$ in $\mathbb{Z}/11\mathbb{Z}$. We have that $x_{n+1} = x_n^2$, and so the sequence is eventually periodic. The first few terms of the sequence are

$$\overline{2}, \overline{4}, \overline{5}, \overline{3}, \overline{9}, \overline{4}, \ldots$$

and will cycle through $(\overline{4}, \overline{5}, \overline{3}, \overline{9})$ from there. Hence, we have that, for all $n \geq 2$, the residue class $\overline{F_n} = x_n + \overline{1}$ cycles through $(\overline{5}, \overline{6}, \overline{4}, \overline{10})$. In particular,

$$F_n \equiv 4 \pmod{11}$$

infinitely often, and 4 is a square modulo 11.

vi) To see that $F_4 = 65537$ is prime, it therefore suffices to show that

$$3^{2^{2^4-1}} = 3^{2^15} \equiv -1 \pmod{65537}$$

which we can compute by repeated squaring in $\mathbb{Z}/65537\mathbb{Z}$:

$$3 \to 9 \to 81 \to 6561 \to -11008 \to -3668 \to 19139 \to \cdots$$
$$\cdots \to 15028 \to 282 \to 13987 \to 8224 \to -8 \to 64 \to 4096 \to -256 \to -1$$

Hence F_4 is prime

vii) Let $p = 2^n + 1$ be a prime for some $n > 2$. As a primitive root exists in $\mathbb{Z}/p\mathbb{Z}$, we can compute the multiplicative order of $\overline{2}$ to be

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

As such,

$$2^{2^{n-1}} \equiv 2^{\frac{p-1}{2}} \equiv 1 \pmod{p} \Rightarrow 2^{2^N} \equiv 1 \pmod{p}$$

for all $N \geq n-1$. Thus $F_N \equiv 2 \pmod{p}$ for all $N \geq n$. But

$$\left(\frac{2}{p}\right) = 1 \text{ if } p \equiv \pm 1 \pmod{8}$$

and $p = 2^n + 1 \equiv 1 \pmod{8}$ for all $n \geq 3$. Thus p cannot be elite, as F_N is a square infinitely often.