1 Primes and Squares

Written by Aditi Talati, Bruce Xu, David Lin.

For the entirety of this problem, assume that p is a *prime* number.

1.1 The rules of mod p arithmetic

In the world of modular arithmetic, we only care about the remainder of a number when dividing by p. We say that a is congruent to b (modulo p) if p divides $a - b$ (sometimes written as $a \equiv b \pmod{p}$). Here are some valid statements we could also say:

- 9 is congruent to 2 (mod 7). 9 *is* 2 (mod 7). 10 *is not* 2 (mod 7).
- -2 is 5 (mod 7), and it is also 12 (mod 7).
- 26 is 5 (mod 7), and 31 is 3 (mod 7), so $26 + 31$ should be $3 + 5$ (mod 7), also known as 1 (mod 7).
- 26×31 is 3×5 (mod 7), which is also 1 (mod 7)
- The set $S = \{0, 1, 7, 8\}$ (mod 7) has size 2. (Equivalently, there are exactly 2 possible remainders obtained from dividing elements of S by 7.)
- $14 \times 5 = 70$ is 0 (mod 7), so we expect one of 14 or 5 to be 0 (mod 7).
- The polynomial $x^2 - 4x + 1$ is $(x + 1)^2$ (mod 3). The polynomial $x^2 - x$ is not 0 (mod 3), even though substituting any integer value of a, $a^2 - a \equiv 0$ (mod 3).

Here is some practice with this idea:

1. Compute the following expressions (mod 7), giving an integer between 0 and 6 (inclusive) as your answer:
   (a) **[1]** $3 + 5$
   (b) **[1]** $2 - 10$
   (c) **[1]** 10×10
   (d) **[1]** 10^{2021}

   Solution to Problem 1:

   (a) (a) 3, (b) 6, (c) 2, (d) 5 (one does this by listing the sequence $1, 10, 10^2, \cdots$ (mod 7) (which is $1, 3, 2, 6, 4, 5, 1, 3, \cdots$, and repeats every 6 terms).

What about division modulo p? Unfortunately, our definitions don't make sense for rational numbers, but we'll show some sense in which division is possible.

2. (a) **[1]** Find an integer k such that $5k \equiv 1$ (mod 7), with $0 \leq k < 7$.
   (b) **[1]** Show that for the above k, $k \cdot (5n) \equiv n$ (mod 7) (and thus this k deserves the name "5^{-1} (mod 7)").

   Solution to Problem 2:

   (a) i. $k = 3$ works, since $5k = 15 \equiv 1$ (mod 7). Any $k \equiv 3$ (mod 7) also works.

ii. $k \cdot (5n) = (5k) \cdot n \equiv n \pmod 7$.

It is true in general that some number deserves the name $a^{-1} \pmod p$, as long as a is not $0 \pmod p$. (We cannot have 0^{-1}!)

3. (a) **[1]** If $a \not\equiv 0 \pmod p$, prove that for any integers x and y, if $ax \equiv ay \pmod p$, then $x \equiv y \pmod p$.

   (b) **[1]** If $a \not\equiv 0 \pmod p$, show that there is some element of P, which we will call b, such that $ab \equiv 1 \pmod p$.

   (Hint. Consider the set $\{0, a, 2a, \cdots, (p-1)a\}$.)

   (c) **[1]** Now we explicitly find one such b. If $a \not\equiv 0 \pmod p$, show that $a^{p-1} \equiv 1 \pmod p$. (This also means that a^{p-2} is $a^{-1} \pmod p$.)

   Hint. Consider the set $\{a, 2a, \cdots, (p-1)a\}$. What is the product?

   (d) **[2]** (Sanity check) Suppose $a, b, c \not\equiv 0 \pmod p$ are positive integers satisfying

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 1$$

   Show that $a^{-1} + b^{-1} + c^{-1} \equiv 1 \pmod p$.

Solution to Problem 3:

(a) i. This boils down to noting that $p \mid ab$ implies either $p \mid a$ or $p \mid b$ (by unique factorization of integers), then setting $b = x - y$.

ii. The map $x \mapsto ax$ is a permutation of $\{1, 2, \cdots, p-1\}$.

iii. $\{1, \cdots, p-1\}$ and $\{a, \cdots, (p-1)a\}$ are the same sets mod p, so by comparing the products:

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

so $a^{p-1} \equiv 1 \pmod p$.

iv. Since $ab + bc + ca = abc$, thus $ab + bc + ca = abc \pmod p$, then multiplying by $a^{-1}b^{-1}c^{-1} \pmod p$ gives us the intended result.

Now we solve an IMO problem. There aren't many points given because IMO problems are easy.

4. (a) **[1]** Define the sequence

$$a_n = 2^n + 3^n + 6^n - 1, \ n \geq 1.$$

   Show that any prime $p \geq 5$ will divide a_{p-2}.

   (b) **[1]** (IMO 2005 Q4) Conclude that the only natural number coprime to every term in the sequence $\{a_n\}$ is 1.

Solution to Problem 4:

(a) i. $a_{p-2} = 2^{p-2} + 3^{p-2} + 6^{p-2} - 1 \equiv 2^{-1} + 3^{-1} + 6^{-1} - 1 \equiv 0 \pmod p$.

ii. We only have to check that all prime numbers are not coprime to every term in the sequence. $p \geq 5$ isn't, due to part (a), and for $p = 2, 3$, $a_2 = 48$.

1.2 Quadratic things

In this section, we try to figure out when something deserves the name $\sqrt{-1} \pmod p$. [1]

5. Assume p is an odd prime. Let's try to partition the elements of $\{1, \cdots, p-1\}$ into sets of the form $\{a, -a, a^{-1}, -a^{-1}\} \pmod p$. As an example, for $p = 7$ we have the sets

$$\{1, 6\}, \{2, 5, 4, 3\}$$

   (a) **[3]** Do this for $p = 5, 11, 13$.

   (b) **[2]** In general, figure out which a causes the set $\{a, -a, a^{-1}, -a^{-1}\} \pmod p$ to have size less than 4.

   (c) **[2]** Show that the solution set of $a^2 + 1 \equiv 0 \pmod p$ has size 0 or 2.

   (d) **[2]** Conclude that the equation $a^2 + 1 \equiv 0 \pmod p$ has a solution if and only if $p \equiv 1 \pmod 4$. (When they exist, these values of a deserve the name $\pm\sqrt{-1}$!)

   Solution to Problem 5:

   (a) i.
   - $p = 5 : \{1, 4\}, \{2, 3\}$
   - $p = 11 : \{1, 10\}, \{2, 5, 6, 9\}, \{3, 4, 7, 8\}$
   - $p = 13 : \{1, 12\}, \{2, 6, 7, 11\}, \{3, 4, 9, 10\}, \{5, 8\}$

   ii. If $a \equiv -a$, then $a \equiv 0$. If $a \equiv a^{-1}$, then $a \equiv \pm 1$. If $a \equiv -a^{-1}$, then $a^2 + 1 \equiv 0$.

   iii. Size at most 2 because a polynomial cannot have more than n distinct roots. If $a \pmod p$ was a root of polynomial $f(x) \pmod p$, then

$$f(x) = (x - a)g(x) + f(a)$$

   for some polynomial g, so $(x - a)$ divides $f(x) \bmod p$.

   It cannot be size 1, because this can't be a double root. (Otherwise, $i = -i$, so $2i = 0$ then $i = 0 \pmod p$.)

   iv. When we partition $\{1, \cdots, p-1\}$, we get one set of 2 containing $\{1, -1\}$, possibly one set of 2 from the roots of $a^2 + 1 \equiv 0$, and many sets of 4. So whether $a^2 + 1 \equiv 0$ has roots depends solely on $(p - 1) \pmod 4$.

Generally, if a number s has a square root $\pm\sqrt{s} \pmod p$, we say that s is a quadratic residue. Likewise, if s doesn't have an appropriate square root then s is a quadratic non-residue.

What about $\sqrt{2} \pmod p$?

6. **[7]** For which p does $a^2 - 2 \equiv 0 \pmod p$ have a solution? As a hint, we would like to start by partitioning the elements of $\{1, \cdots, p-1\}$ into sets of the form

$$\left\{a, -a, \frac{1}{a}, -\frac{1}{a}, \frac{a+1}{a-1}, -\frac{a+1}{a-1}, \frac{a-1}{a+1}, -\frac{a-1}{a+1}\right\} \pmod p$$

   where we omit the degenerate elements that are 0 or divide by 0.

   Solution to Problem 6: We first consider when this set has size smaller than 8:

[1] Technically, we only ever know if it is either $\sqrt{-1}$ or $-\sqrt{-1}$.

- $a = \pm 1$: $\{\pm 1\}$
- $a = \pm\sqrt{-1}$: $\{\pm\sqrt{-1}\}$
- $a = 1 \pm \sqrt{2}$: $\{\pm 1 \pm \sqrt{2}\}$

Our analysis leads us to consider cases mod 8:

- 1 mod 8: $\sqrt{-1}$ exists. So $p - 1 = 4 + (4) + 8k$, so it is a quadratic residue.
- 3 mod 8: $\sqrt{-1}$ doesn't exist, so $p - 1 = 2 + (4) + 8k$. It is not a quadratic residue.
- 5 mod 8: $\sqrt{-1}$ exists, so $p - 1 = 4 + (4) + 8k$ so 2 is not a quadratic residue.
- 7 mod 8: $\sqrt{-1}$ doesn't exist, so $p - 1 = 2 + (4) + 8k$. 2 is a quadratic residue.

1.3 Fermat's two square theorem, via windmills

Surprisingly, we can use "grouping" techniques in contexts that aren't purely modulo p. Here, we will show Fermat's two-square theorem...

Theorem. (Fermat) If $p \equiv 1 \pmod 4$, then p can be expressed as the sum of two perfect squares.

...using windmills!

7. **[7]** An **integer rectangle** is a rectangle whose side-lengths are integers. A **windmill** is a shape formed by removing 4 congruent integer rectangles from an integer square at the corners such that the resulting shape is rotationally-symmetric. A **blade partition** of a windmill is a rotationally-symmetric way to cut it into a square and 4 congruent rectangles. (A windmill may have more than one blade partition!)

Consider all windmills of area p. Show that the total sum of the number of blade partitions among these windmills is odd. Conclude Fermat's two-square theorem.

Solution to Problem 7: Each windmill admits two blade partitions, except one whose central square is aligned with the 4 congruent rectangles (the "blades"). In this case, the sidelength of the central square divides the area, so it is 1. Thus, there is exactly one such windmill with a single blade partition.

On the other hand, we can flip the axes of all the blades simultaneously. This produces a pairing between blade partitions except for when the blades are square, of which there are an odd number of cases. But any such case gives a representation of p as the sum of two perfect squares!

2 Around and around

Written by Zhao Yu Ma, David Lin.

2.1 Introduction

In this section, we will be looking at the winding number of a loop around the origin.

A **loop** is a path not passing through the origin that returns to where it started off. More rigorously, we define it as a continuous function $\gamma : [0, 2\pi] \to \mathbb{C} - \{0\}$ such that $\gamma(0) = \gamma(2\pi)$.

Intuitively, the **winding number** of a path γ is the total number of times that the loop travels counter-clockwise around the origin. The winding number is denoted as $w(\gamma)$.

If we imagine a loop as a slack rope tied around a pillar (going from the floor to the ceiling), then it is clear that without untying or cutting the rope, the number of times that the rope winds around the pillar must stay constant. In mathematical terms, winding number is preserved under "continuous deformation".

2.2 An integral formula

Here, we give an explicit formula for the winding number.

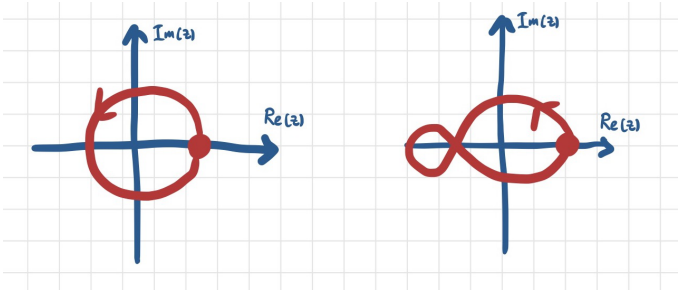
One approach is as follows: define a continuous[2] function $\theta : [0, 2\pi] \to \mathbb{R}$ where

$$\theta(s) \equiv \arg(\gamma(s)) \pmod{2\pi}, \qquad \theta(0) = 0$$

In words, θ is the angle between a ray pointing in the direction of $\gamma(s)$ and the positive x-axis. Then, the angle that this ray rotates around the origin will be $\theta(2\pi)$. Dividing this by 2π yields the winding number.

Let's try out an example to see how this works.

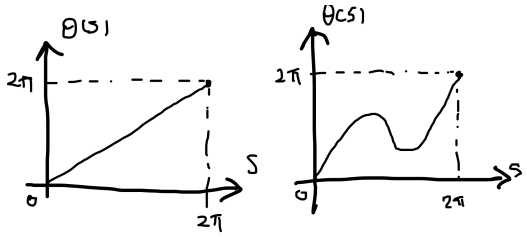
8. **[2]** Sketch the functions $\theta(s)$ for a loop around a unit circle, and a figure 8, where origin is in one of the holes. (Keep in mind that you should be able to draw the graphs without lifting your pen off the paper!)



Show that the winding number of both loops are the same.

Solution to Problem 8: It is clear from this sketch that both loops have winding number 1.

[2]For the purposes of this section, this means that you can draw the graph of θ without lifting your pen off the paper. An implication is that θ is well-defined (even though we will only define it modulo 2π).



Our earlier intuition about continuous deformation tells us why this is the case: the figure 8 can continuously deform to the unit loop, so they must share the same winding number.

If γ is differentiable[3] (i.e. the derivative $\gamma'(s) = \frac{d}{ds}\gamma(s) = \lim_{h\to 0} \frac{\gamma(s+h)-\gamma(s)}{h}$ exists), we can also come up with the following equation for the winding number

$$w(\gamma) = \frac{1}{2\pi i}\int_0^{2\pi} \frac{\gamma'(s)}{\gamma(s)} ds. \tag{1}$$

9. (a) **[1]** Show that $e^{i\theta(s)} = \frac{\gamma(s)}{|\gamma(s)|}$.

   (b) **[2]** Assuming that θ is differentiable, show that $i\theta'(s) = \frac{\gamma'(s)}{\gamma(s)} - \frac{|\gamma(s)|'}{|\gamma(s)|}$.

   (c) **[2]** Prove equation (1) assuming both γ, θ are differentiable. Recall that w is the number of times that γ winds around the origin. *(Hint. How do you read off w from the graph of θ?)*

   Solution to Problem 9:

   (a) In general we have $z = |z| \cdot \arg(z)$, then substitute $z = \gamma(s)$.

   (b) Differentiate both sides of the previous part.

   (c) Integrate from 0 to 2π, and note that $\int \frac{f'}{f} = \log f$ for real nonvanishing f.

Here are some properties of winding numbers, that we will be using frequently in the later sections. **Use equation (1)** to prove the following:

10. (a) **[2]** Let $f : [0, 2\pi] \to \mathbb{C} - \{0\}$ be a loop. Show that $w(\frac{1}{f}) = -w(f)$.

    (b) **[2]** Let $f, g, h : [0, 2\pi] \to \mathbb{C} - \{0\}$ be loops. If $h(z) = g(z)f(z)$, Show that $w(h) = w(g) + w(f)$.

    Solution to Problem 10:

    (a) Chain rule using eqn (1).

    (b) Product rule using eqn (1).

Given real $r \geq 0$, let $\gamma_r(\theta) = re^{i\theta}$ be the loop of radius r clockwise around the origin. We will often be looking at paths of the form γ_r, as well as composition of functions with γ_r.

11. **[2]** Let $f(z) = \frac{1}{z}$. **Using equation (1)**, calculate the winding numbers $w(\gamma_r)$, $w(f \circ \gamma_r)$ for $r > 0$.

    Solution to Problem 11: Answer: $w(\gamma_r) = 1, w(f \circ \gamma_r) = -1$.

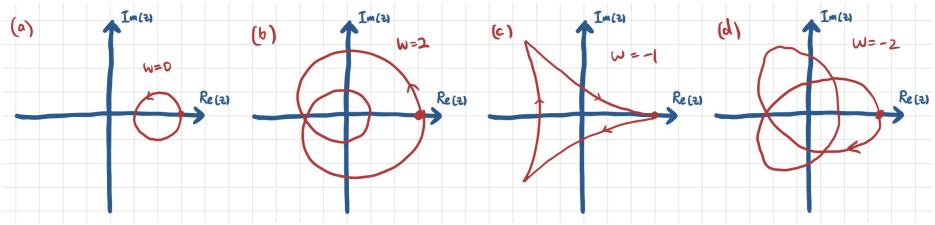
[3]strictly speaking, γ should be continuously differentiable, i.e. γ' should also be continuous.

$$\begin{aligned} w(\gamma_r) &= \frac{1}{2\pi i}\int_0^{2\pi} \frac{(re^{is})'}{re^{is}} ds \\ &= \frac{1}{2\pi i}\int_0^{2\pi} i\, ds = 1 \\ w(f\circ\gamma_r) &= \frac{1}{2\pi i}\int_0^{2\pi} \frac{(re^{-is})'}{re^{-is}} ds \\ &= \frac{1}{2\pi i}\int_0^{2\pi} (-i)\, ds = -1 \end{aligned}$$

Usually, we do not use equation (1) to calculate the winding number every time as that is too tedious. **From now on, unless otherwise stated, you may intuitively justify the values of any winding number** (as the number of times the loop travels counter-clockwise around the origin).

12. Sketch $f\circ\gamma_1$ for each of the following functions, and deduce the winding number $w(f\circ\gamma_1)$.
    (a) **[1]** $z+2$
    (b) **[1]** $2z^2+z$
    (c) **[1]** $z^2+\frac{2}{z}$
    (d) **[1]** $z+\frac{2}{z^2}$

Solution to Problem 12:



2.3 A winding problem

13. As an application, we would like to show that all the roots of the polynomial $9z^8+8iz^7+8iz-9$ lie on the unit circle centered around the origin ($|z|=1$).
    (a) **[2]** Show that if $|z|=1$, then $|9z^8+8iz^7| = |8iz-9|$.
    (b) **[3]** Let $f(z)=z^7$, $g(z)=9z+8i$, $h(z)=8iz-9$. Sketch the loops $f\circ\gamma_1, g\circ\gamma_1, h\circ\gamma_1$, and deduce their respective winding numbers $w(f\circ\gamma_1), w(g\circ\gamma_1), w(h\circ\gamma_1)$.
    (c) **[1]** Let $k(z)=\frac{9z^8+8iz^7}{8iz-9}$. Calculate the winding number $w(k\circ\gamma_1)$.
    (d) **[1]** Show that there are at least 8 distinct roots when $|z|=1$, and prove the problem statement.

Solution to Problem 13:

(a) Use $\overline{z} = z^{-1}$, so $|9z^8 + 8iz^7| = |z|^8 \cdot |9 + 8iz^{-1}| = |9 - 8iz|$.

(b) $w(f \circ \gamma_1) = 7, w(g \circ \gamma_1) = 1, w(h \circ \gamma_1) = 0$.

(c) $w = 7 + 1 - 0 = 8$.

(d) A winding number of 8 means that for at least 8 distinct values $0 = s_1, s_2, \cdots, s_8$ on $[0, 2\pi)$, we must have $\arg k(\gamma_1(s_i)) \equiv 0 \pmod{2\pi}$. But $|k(z)| = 1$, so this means that $k(\gamma_1(s_i)) = 1$, so $\gamma_1(s_i)$ are (distinct) roots of the original polynomial.

2.4 Fundamental theorem of algebra

We will prove the fundamental theorem of algebra, which states that every non-constant single-variable polynomial with complex coefficients has at least one complex root

For simplicity, we will prove it for our favorite cubic polynomial $p(z) = z^3 + 4z^2 + 17z + 2021$. Assume the contrary, that $p(z)$ has no (complex) root.

14. (a) **[3]** Write $p(z) = z^3 f(z)$. Show that for sufficiently large r, $\text{Re}(f \circ \gamma_r) > 0$. Sketch $f \circ \gamma_r$ and deduce the winding number $w(f \circ \gamma_r)$, and $w(p \circ \gamma_r)$.

(b) **[2]** In a similar way, find the winding number $w(p \circ \gamma_0)$. (Hint: your answers for $w(p \circ \gamma_r)$ and $w(p \circ \gamma_0)$ should be different.)

However, we can continuously deform $p \circ \gamma_r$ to $p \circ \gamma_0$ by gradually decreasing r to 0. We know that the winding number is invariant under continuous deformation, so this leads to a contradiction, which finishes the proof.

Here is a quick concept check:

(c) **[1]** Why did we need the assumption that $p(z)$ has no root?

Solution to Problem 14:

(a) f looks like $1 + \frac{A}{z} + \frac{B}{z^2} + \frac{C}{z^3}$, so sufficiently large r makes $f \circ \gamma_r$ sufficiently close to 1 on any value, so the real part is positive and $f \circ \gamma_r$ has no winding, so $w(p \circ \gamma_r) = -3$.

(b) This has 0 winding, since it's constant.

(c) If p had a root z, then $p \circ \gamma_{|z|}$ passes through 0 and is not a valid loop around the origin.

2.5 Brouwer's fixed point theorem

We will look at Brouwer's fixed point theorem which states that given a closed disk $D = \{z \mid |z| \leq 1\}$ and a **continuous** function $f : D \to D$, there exists a point $z \in D$ such that $f(z) = z$.

15. **[1]** To get a feel of what this theorem is saying, we show that a slight modification is false. Construct a continuous function $f : D \setminus \{0\} \to D \setminus \{0\}$ such that for every point $z \in D \setminus \{0\}$, $f(z) \neq z$.

Solution to Problem 15: Any rotation should work.

16. Let's prove the theorem. Like the previous section, we start off by assuming that there is no such fixed point, which means that $f(z) \neq z$ for all $z \in D$. This means that we may draw a ray from z to $f(z)$, which intersects the unit circle again at $g(z)$.

Just like the previous parts, we will compute two different values for $w(g \circ \gamma_r)$.

(a) **[2]** Find $w(g \circ \gamma_1)$.

(b) **[1]** Find $w(g \circ \gamma_0)$.

These two values are different! We want to continuously deform $g \circ \gamma_1$ to $g \circ \gamma_0$. However, to do this, we need the condition that g is a continuous function, which we will prove here.

(c) **[3]** Let $z = a + bi$, $f(z) = c + di$. Write $g(z) = f(z) + \lambda(z - f(z))$ where $\lambda \in \mathbb{R}_{\geq 0}$. Find an expression for λ in terms of a, b, c, d. (It will involve polynomials of a, b, c, d, and square-roots.) Argue that the term in the square-root is never negative. (The resulting function will be continuous in z and $f(z)$!)

This means that λ is continuous in the two variables $z, f(z)$. Since $f(z)$ is also continuous in z, we can conclude that $g(z)$ is continuous.

Now, we can continuously deform $g \circ \gamma_1$ to $g \circ \gamma_0$, so the winding numbers for must be the same, leading to a contradiction.

A final question:

(d) **[1]** Where exactly in the argument did we use the assumption that f has no fixed point?

Solution to Problem 16:

(a) $w(g \circ \gamma_1) = 1$. This is because $g(z) \neq z$.

(b) As usual, this is 0.

(c)
$$\lambda = \frac{-B + \sqrt{B^2 - 4AC}}{2A}$$
where $A = (a-c)^2 + (b-d)^2$, $B = a(c-a) + b(d-b)$, $C = a^2 + b^2 - 1$. $B^2 - 4AC \geq 0$ because $A \geq 0$ and $C \leq 0$.

(d) If not we can't draw the ray to define $g(z)$!

2.6 Sperner's lemma

Sperner's lemma is the discrete, combinatorial analog of Brouwer's fixed point theorem. In fact, both theorems are equivalent!

Theorem. (Sperner's Lemma) Given a triangle ABC, and a **triangulation**[4] T of the triangle, the set S of vertices of T is colored with three colors (labelled r, g, y) satisfying the following conditions:

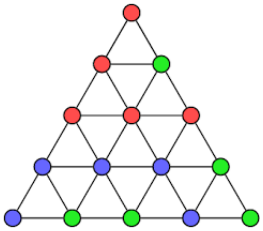
(1) Every vertex on side AB is colored r or g,

(2) Every vertex on side AC is colored r or y,

(3) Every vertex on side BC is colored g or y.

Then, there exists a triangle from T, whose vertices are colored with the three different colors.

[4] A triangulation of a figure is a partition of the figure into triangles such that the intersection between any two triangles is either empty, a single vertex or an entire edge (for both triangles).



17. **[5]** Prove Sperner's lemma.

(Hint. The main idea is extremely similar to the proof of Brouwer's fixed point theorem! Associate the colors r, g, y to the points $1, e^{2\pi i/3}, e^{4\pi i/3}$ in $\mathbb{C} - \{0\}$. Can you define a discrete version of winding number? What about a discrete version of continuous deformation?)

Solution to Problem 17: Given a sequence of colors from r, g, y whose first and last colors are the same, we can define a winding number by associating them with the points $1, e^{2\pi i/3}, e^{4\pi i/3}$ in $\mathbb{C} - \{0\}$ and moving linearly between them. So the perimeter of ABC has winding number ± 1, and each triangle has winding 0.

Now assuming each triangle has winding 0, we either argue that (1) winding doesn't change under "deformation", which is adding or removing a vertex from our path or (2) the total winding along the perimeter should just be the sum of winding numbers of each triangle.

3 Cyclotomic Polynomials

Written by Bruce Xu, David Lin.

The section will be centered around cyclotomic polynomials, which play an important role in number theory (in particular algebraic number theory), Galois Theory and Geometry. There are many ways that these polynomials can be introduced, and this exposition offers only one perspective. We will define, motivate and build up to some important results about these polynomials.

3.1 Euler's Totient Function

The notion of being *relatively prime* is central in the study of numbers. Heuristically speaking, when we analyse structures that are relatively prime to each other, this gets rid of all of the unnecessary "fluff" and "padding" of the problem.

18. (a) **[3]** Let $\phi(n)$ denote the number of integers k that are less than or equal to n such that n and k are relatively prime. Calculate $\phi(5)$, $\phi(15)$, $\phi(45)$.

    (b) **[2]** Find and prove a general formula for $\phi(n)$ if $n = p_1^{k_1}p_2^{k_2}...p_l^{k_l}$ is the prime factorization of n.

    Solution to Problem 18:

    (a) $\phi(5) = 4, \phi(15) = 8, \phi(45) = 24$.

    (b) $\phi(n) = \prod_{i=1}^{\ell}(p_i - 1)p_i^{k_1-1}$. The case $\phi(p^k)$ is easy, since being relatively prime to p^k is exactly being not divisible by p. Now we show that $\phi(mn) = \phi(m)\phi(n)$ for m, n coprime using CRT.

19. Consider the fractions:
$$\frac{1}{n}, \frac{2}{n}, ..., \frac{n}{n}$$
Reduce them to their most primitive form (i.e. the numerator and denominator are coprime).

    (a) **[1]** How many fractions are there for each given denominator, and how many denominators are there?

    (b) **[1]** Prove that $\sum_{d|n}\phi(d) = n$.

    Solution to Problem 19:

    (a) There are exactly $\phi(n)$ distinct denominators, which represent the number of integers $m \leq n$ that are relatively prime to n.

    (b) There are $\phi(n/d)$ fractions with denominator d.

20. **[2]** A place that the ϕ function shows up is Euler's Theorem, which is an extension of Fermat's Little theorem. Prove that for coprime integers a and n:
$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

    Solution to Problem 20: The idea is almost identical to demonstrating Fermat's Little Theorem: consider the bijection $x \mapsto ax$ on $(\mathbb{Z}/n\mathbb{Z})^\times$ to itself (i.e. residues mod n that are coprime to n), then take the product across all values of $x \in (\mathbb{Z}/n\mathbb{Z})^\times$.

3.2 Towards Cyclotomic Polynomials

The difference of squares factorisation is ubiquitous in many areas of mathematics.

$$x^2 - 1 = (x + 1)(x - 1)$$

So is the factorisation of $x^3 - 1$:

$$x^3 - 1 = (x - 1)(x^2 + x + 1)$$

Going furhter, we can write $x^n - 1$ as a product of **integer polynomials** (polynomials with integer coefficients) for larger and larger n:

$$x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x^2 + 1)$$
$$x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$$
$$\cdots$$

We see that at each successively higher power, we are introducing brand new polynomials. Just as how we decompose $n = 0, 1, 2, 3, \cdots$ into prime factors, we are now moving towards decomposing polynomials $x^n - 1 = x - 1, x^2 - 1, x^3 - 1, \cdots$ into "prime" (irreducible) polynomials. We could imagine giving these polynomial names:

$$x^3 - 1 = \Phi_1(x)\Phi_3(x)$$

$$x^4 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)$$

This is, however, not a rigorous definition. For that, we can think about what happens if we allow factorization using complex coefficients. The polynomial $x^n - 1$ has n distinct complex roots given by $\{e^{2\pi ik/n}\}_{k=0,1,2,\cdots,n-1}$, so it admits the factorization

$$x^n - 1 = (x - 1)(x - \zeta_n^1) \cdots (x - \zeta_n^{n-1})$$

where $\zeta_n = e^{2\pi i/n}$. We see that the new (yet undefined) Φ_n must be a product of some subset of these factors.

Define the n-th **cyclotomic polynomial** as the following:

$$\Phi_n(x) = (x - \zeta_1)(x - \zeta_2)...(x - \zeta_k)$$

where $\zeta_1, \zeta_2, ..., \zeta_k$ are all of the the n-th primitive roots of unity. Recall that complex number z is an n-th **root of unity** if and only if $z^n = 1$. Furthermore, we see that z is a **primitive** n-th root of unity if $z^m \neq 1$ for all $m = 1, 2, 3, ..., n - 1$.

21. For two **monic** integer polynomials $f(x), g(x)$ (i.e. their leading coefficient is 1), define their **greatest common divisor of two polynomials** to be the monic polynomial $h(x)$ of the maximal degree that divides both $f(x)$ and $g(x)$.

    (a) **[2]** Show that the greatest common divisor of the polynomials $x^a - 1$ and $x^b - 1$ is equal to $x^{\gcd(a,b)} - 1$.

    (b) **[3]** Factor $x^7 - 1$, $x^{12} - 1$, $x^{27} - 1$ completely into integer polynomials.

    Solution to Problem 21:

(a) Note that if $a > b$, then $(x^a - 1, x^b - 1) = (x^b(x^{a-b} - 1), x^b - 1) = (x^{a-b} - 1, x^b - 1)$, so we can run the Euclidean Algorithm until we reach the gcd.

(b)

$$x^7 - 1 = (x - 1)(x^6 + x^5 + \cdots + 1)$$
$$x^{12} - 1 = (x - 1)(x + 1)(x^2 + 1)(x^2 + x + 1)(x^2 - x + 1)(x^4 - x^2 + 1)$$
$$x^{27} - 1 = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1)(x^{18} + x^9 + 1)$$

22. (a) **[1]** Describe a bijection between the fractions in $\frac{1}{n}, \frac{2}{n}, ..., \frac{n}{n}$ and n-th roots of unity such that a (reduced) fraction with denominator d is mapped to a primitive d-th root of unity.

(b) **[2]** Prove that $\prod_{d|n} \Phi_d(x) = x^n - 1$.

Solution to Problem 22:

(a) k/n goes to ζ^k where ζ is a fixed primitive n-th root of unity.

(b) Let ζ be a primitive n-th root of unity. Then $x^n - 1$ factors like

$$x^n - 1 = (x - \zeta)(x - \zeta^2) \cdots (x - \zeta^n)$$

So by gathering the ζ^m's for which $(\zeta^m)^d = 1$, we should get all the primitive d-th roots of unity. Therefore we conclude that

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

23. **[2]** Demonstrate that the n-th cyclotomic polynomial $\Phi_n(x)$ is the largest (by degree) polynomial that divides $x^n - 1$ but is coprime[5] to each $x^k - 1$ for any $k < n$.

Solution to Problem 23: Let ζ be a primitive n-th root of unity. Then $x^n - 1$ factors like

$$x^n - 1 = (x - \zeta)(x - \zeta^2) \cdots (x - \zeta^n).$$

If $(\zeta^d)^k = 1$ for some $k < n$ then $(x - \zeta^d)$ divides $x^k - 1$. Otherwise, ζ^d is a primitive n-th root of unity so it divides $\Phi_n(x)$. The conclusion follows.

24. (a) **[3]** Find $\Phi_7(x)$, $\Phi_{12}(x)$, $\Phi_{27}(x)$.

(b) **[2]** Write a general formula for $\Phi_p(x)$, where p is a prime number. What about $\Phi_{p^k}(x)$?

(c) **[2]** Similarly, find a general formula for $\Phi_{2p}(x)$ and subsequently $\Phi_{2^k p}(x)$ where p is a prime number and k is a non-negative integer.

(d) **[1]** Now find a general form for the polynomial $\Phi_{p^k m}(x)$ where p does not divide m in terms of $\Phi_m(x)$.

Solution to Problem 24:

(a)

$$\Phi_7(x) = x^6 + x^5 + \cdots + 1$$
$$\Phi_{12}(x) = x^4 - x^2 + 1$$
$$\Phi_{27}(x) = x^{18} + x^9 + 1$$

[5]Two monic integer polynomials are coprime if the only monic integer polynomial that simultaneously divides both is 1.

(b) $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + 1$, $\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}})$.

(c) $\Phi_{2p}(x) = \Phi_p(-x), \Phi_{2p^k}(x) = \Phi_{p^k}(-x)$.

(d) $\Phi_{p^k m}(x) = \Phi_m(x^{p^k})/\Phi_m(x^{p^{k-1}})$.

25. **[3]** It seems that we have taken for granted that Cyclotomic Polynomials are guaranteed to have integer coefficients. Prove that this fact holds for all $\Phi_n(x)$.

Solution to Problem 25: We proceed by induction. $n = 1$ is obvious. Then, for $n \geq 2$,

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d<n, d|n} \Phi_d(x)}$$

It remains to show that if the quotient of two monic polynomials with $\mathbb{Z}$-coefficients is a polynomial, then it is a monic polynomial with $\mathbb{Z}$-coefficients. This is easy by long division.

26. (a) **[1]** Factorize $x^4 + x^2 + 1$. *(Hint. Add and subtract x^2.)*

(b) **[3]** Factor $\Phi_n(x^k)$ into cyclotomic polynomials of x.

Solution to Problem 26:

(a) Difference of two squares yields $x^4+2x^2+1-x^2 = (x^2+1)^2-x^2 = (x^2+x+1)(x^2-x+1)$

(b) $\Phi_n(x^k) = \prod_{d|k} \Phi_{dn}(x^k)$

27. **[2]** Demonstrate that for any a positive integer $n > 1$, it is the case that $\Phi_n(1) = 1$ if n is not a prime power and $\Phi_n(1) = p$ if n is a prime power of p *(Hint. Induction!)*

Solution to Problem 27: We will use that

$$n = \frac{x^n - 1}{x - 1}|_{x=1} = \prod_{d|n, d>1} \Phi_d(1)$$

Then the conclusion follows immediately from induction.

Surprisingly, we are already able to prove some nontrivial statements that don't explicitly involve cyclotomic polynomials. Here is one example:

28. **[5]** Show that there are infinitely many n such that every prime factor of $2^n - 1$ is at most $2^{n/2021}$.

Solution to Problem 28: Magnitude bound gives that $\Phi_n(x) \leq (|x| + 1)^{\varphi(n)}$, and there are infinitely many n such that $\varphi(n) \ll cn$.

3.3 Irreducibility

So far, we've managed to express $x^n - 1$ as a product of cyclotomic polynomials:

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

This begs the question: can we factorize this any further? In this section, we show that the answer is no: $\Phi_n(x)$ is **irreducible**, which means that it is not the product of two (non-constant) integer

polynomials. This concept should remind you of the prime numbers among the natural numbers; irreducible polynomials are the "primes" among polynomials.

Showing polynomials are irreducible isn't easy. Have a stab at one example of it:

29. **[5]** Show that $x^5 - x - 1$ is irreducible. *(Hint. Suppose you can factor it as $f(x)g(x)$. If f is linear, then it is $x \pm 1$, which can't happen. Otherwise, f is quadratic and g is cubic, and the constant terms are $1, -1$ respectively. What can you say about the other coefficients?)*

Solution to Problem 29: If $x^5 - x - 1$ has a linear factor, then it is $x \pm 1$, but by substituting $x = \pm 1$ we check that neither of these are linear factors.

We are left with two cases:

- $x^5 - x - 1 = (x^2 + ax + 1)(x^3 + bx^2 + cx - 1)$. Then $a + b = 0, ab + 1 = 0, b + ac - 1 = 0, c - a = -1$. Writing everything in terms of a, we get $a^2 = 1, -a + (a-1)a - 1 = 0$, which is impossible.
- $x^5 - x - 1 = (x^2 + ax - 1)(x^3 + bx^2 + cx + 1)$. Then $a + b = 0, ab - 1 = 0$, which is impossible.

In general, we can't just get by brute-force case consideration. There are some other methods (for instance, looking at the size of the complex roots), but we'll look at one in particular, which is to think about polynomials "mod p". We recap some usual notions of polynomials mod p:

- The polynomial $x^2 - 4x + 1$ is $(x+1)^2 \pmod 3$. The polynomial $x^3 - x$ is not $0 \pmod 3$, even though substituting any integer value of a, $a^3 - a \equiv 0 \pmod 3$.
- $3x^2 + 3x + 1$ is constant (mod 3) because it is $1 \pmod 3$. The degree of $3x^2 + x + 1 \pmod 3$ is 1, but the degree of $3x^2 + x + 1$ is 2.

We will first show that $\Phi_p(x)$ is irreducible for prime p. Recall that $\Phi_p(x) = \frac{x^p - 1}{x - 1}$.

30. (a) **[2]** Show that $\Phi_p(x) \equiv (x-1)^{p-1} \pmod p$. *(Hint. It might be easier to first show that $x^p - 1 \equiv (x-1)^p \pmod p$)*

    (b) **[3]** (Eisenstein's Criterion) Suppose $f(y)g(y) \equiv y^{p-1} \pmod p$, and f, g are monic and nonconstant mod p. Conclude that the constant term of $f(y)g(y)$ is divisible by p^2.

    (c) **[1]** Conclude that $\Phi_p(x)$ is irreducible. *(Hint. We've computed the constant term of $\Phi_p(y+1)$ before! Where?)*

Solution to Problem 30:

(a) $x^p - 1 \equiv (x-1)^p \pmod p$ by binomial expansion, and division works. Alternatively, reason that by Wilson's theorem, $\binom{p-1}{k} \equiv (-1)^k \pmod p$.

(b) Consider the lowest term with nonzero coefficient of $f(y)g(y) \pmod p$. This must be y^{p-1} itself, so if f, g are both not constant mod p then they are of the form $y^k, y^{p-1-k} \pmod p$. But that means that the constant terms of f, g are divisible by p, so the constant term of $f(y)g(y)$ is divisible by p^2.

(c) Set $x = y - 1$, then the constant term is $\Phi_p(1) = p$, contradicting the above point if $\Phi_p(x)$ was the product of two nonconstant polynomials.

Showing that all cyclotomic polynomials are irreducible is far more difficult, and the same trick doesn't work. Strangely enough, we will still be considering mod p, but in a completely different way. The following proof is due to Landau:

31. Let f be any irreducible polynomial dividing $x^n - 1$, and p be a prime that does not divide n. We will show that $f(x)$ **divides**[6] $f(x^k)$ for all k coprime to n.

    (a) **[2]** Check that this is true for $f = \Phi_n$ (even though we don't know it's irreducible yet).

    Somehow, this is easier if we assume that k is a large prime p. Here is (informally) why (that $f(x)$ divides $f(x^p)$ for any large prime p):

    - If ζ is a root of $f(x)$ (by assumption, one of the n-th roots of unity), then we just need $f(\zeta^p) = 0$.
    - But $f(\zeta^p) \equiv f(\zeta)^p = 0 \pmod{p}$, so p divides $f(\zeta^p) = f(\zeta^{p \bmod n})$, which is "small", so for large enough p, $f(\zeta^p) = 0$.

    This is not meant to be a real proof (there are many badly defined things!) but we will make this rigorous by considering polynomials.

    (b) **[2]** Show that for prime p, p divides $f(x^p) - (f(x))^p$.

    (c) **[2]** Now suppose $p \equiv k \pmod{n}$, $0 \le k \le n-1$. Then, show that

    $$f(x^p) - f(x)^p \equiv f(x^k) \pmod{f(x)}.$$[7]

    (d) **[3]** Suppose $pg(x) \equiv h(x) \pmod{f(x)}$ where g, h are integer polynomials, and furthermore $\deg h < \deg f$. (By assumption, f is monic.) Show that p divides h.

    (e) **[3]** Show that for integer polynomials h, f (with f monic), if $h(x)$ is a multiple of $p \pmod{f(x)}$ for infinitely many primes p, then f divides h. Conclude that $f(x)$ divides $f(x^p)$ for all large primes p. (Do not assume Dirichlet's theorem on primes in arithmetic progressions.)

    (f) **[3]** Show that for any k coprime to n, we can pick some $N \equiv k \pmod{n}$ such that it does not have any prime factors smaller than C. Conclude that $f(x)$ divides $f(x^k)$ for any k coprime to n.

    This means that if an irreducible f dividing $x^n - 1$ has a primitive n-th root of unity ζ as a root, then it must also have every ζ^k as a root, for any k coprime to n. Hence $\Phi_n(x)$ divides $f(x)$ and so Φ_n is irreducible.

    Solution to Problem 31:

    (a) We know $\Phi_n(x)$ divides $x^{nk} - 1 = \prod_{d|n} \Phi_d(x^k)$, but it cannot divide $x^{mk} - 1$ for $m < n$ (otherwise it also divides $x^{(mk,n)} - 1$), so it divides $\Phi_n(x^k)$.

    (b) Induct using $(a+b)^p \equiv a^p + b^p \pmod{p}$ from binomial theorem.

    (c) $f(x) \mid x^n - 1 \mid (x^p - x^k) \mid f(x^p) - f(x^k)$

[6] This means that there exists an integer polynomial $g(x)$ such that $f(x^k) = g(x)f(x)$.

[7] We write $g(x) \equiv h(x) \pmod{f(x)}$ if $f(x)$ divides $g(x) - h(x)$.

(d) Suppose $pg(x) = q(x)f(x) + h(x)$, then the leading coeffiicent of $q(x) \pmod p$ must be $0 \pmod p$, so $p \mid q(x)$ and hence $p \mid h(x)$.

(e) Write $h(x) = q(x)f(x) + r(x)$ where $\deg r < \deg f$, then $p \mid r(x)$ from the previous part. If this were true for infinitely many primes p, then $r = 0$, so f divides h.

The conclusion falls out from part (c), since if there were infinitely many primes $\equiv k \pmod n$, then $f(x) \mid f(x^k) \equiv f(x^p) \pmod k$.

(f) Directly construct

$$N = n \cdot \prod_{p \le C, p \nmid k} p + k$$

If this factors as $N = q_1 q_2 \cdots q_k$, then $f(x) \mid f(x^{q_1}) \mid f(x^{q_1 q_2}) \mid \cdots \mid f(x^N)$. But $f(x) \mid x^k - x^N$, so $f(x) \mid f(x^k) - f(x^N)$ so the conclusion holds.

Thus, we will have successfully factorized $x^n - 1$ into irreducible polynomials. Not only that, the fact that Φ_n is irreducible means that all the primitive n-th roots of unity are "algebraically indistinguishable". Here is the practical implication you should remember.

32. (a) **[1]** If ζ is a primitive n-th root of unity, and $P(\zeta_n) = Q(\zeta_n)$ for integer polynomials P, Q, then $P(\zeta_n^k) = Q(\zeta_n^k)$ for all k coprime to n. (You might already be familiar with the case $n = 4$!)

(b) **[5]** Show that there are only finitely many n for which the sum of k primitive n-th roots of unity is a nonzero integer.

Solution to Problem 32:

(a) The irreducibility of Φ_n implies $\Phi_n \mid P - Q$.

(b) Write the sum of k primitive n-th roots as a polynomial P of ζ_n. Then, evaluating

$$\sum_{(k,n)=1, 0<k<n} P(\zeta_n^k) = m$$

gives $k \cdot \mu(n) = m \cdot \phi(n)$, so $\phi(n) \mid k$.

3.4 Arithmetic Functions and Möbius inversion

Back to the equation

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x).$$

This gives a recursive formula for Φ_n, but one can't help but wonder if it were possible to get a direct formula.

Here, we consider the related setting where we have two functions $f, F : \mathbb{N} \to \mathbb{R}$, where F is defined by

$$F(n) = \sum_{d \mid n} f(n).$$

Could we recover f from F? Perhaps! If τ is the number of divisors of n, then given the values of F, we will have a system of τ equations in the τ variables $\{f(d)\}_{d \mid n}$. With some luck, this is solvable!

33. It turns out that this is always solvable. Suppose that for m dividing n,

$$f(m) = \sum_{d|n} c_{n,d,m} F(d)$$

(a) **[2]** For $n = 12$, write down these equations for all m dividing n. (Your $c_{n,d,m}$'s should be replaced by actual numbers! For instance, for $n = 2$, we expect the two equations $f(1) = F(1)$ and $f(2) = F(2) - F(1)$.)

(b) **[1]** In general, why is this always solvable?

(c) **[1]** Argue that $c_{n,d,m}$ does not depend on n (and thus we may write it as $c_{d,m}$).

(d) **[3]** Argue that $c_{d,m}$ only depends on m/d (so $c_{d,m} = \mu(m/d)$ for a function μ). Describe the function μ. *(Hint. Try out small values!)*

Solution to Problem 33:

(a)

$$\begin{aligned} f(1) &= F(1) \\ f(2) &= F(2) - F(1) \\ f(3) &= F(3) - F(1) \\ f(4) &= F(4) - F(2) + F(1) \\ f(6) &= F(6) - F(3) - F(2) + F(1) \\ f(12) &= F(12) - F(6) - F(4) + F(2) \end{aligned}$$

(b) Because there's a recursion.

(c) Because regardless of n, we always only need $\{F(d)\}_{d|m}$ to recover $f(m)$, and using the same coefficients.

(d) Consider the function

$$f_d(x) = \begin{cases} f(x/d) & \text{if } d \mid x \\ 0 & \text{otherwise} \end{cases}$$

This means that $F_d(m) = \sum_{e|m} f_d(e)$, but this also means that $c_{d,m} = c_{1,m/d}$.

μ is, of course, the Möbius function, defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n \text{ is square-free with an even number of prime factors} \\ -1 & \text{if } n \text{ is square-free with an odd number of prime factors} \\ 0 & \text{if } n \text{ is not square-free} \end{cases}$$

The formula

$$f(n) = \sum_{d|n} \mu(n/d) F(n)$$

has a name: the **Möbius inversion formula**.

34. Here are some fun applications:

(a) **[2]** (Euler's Totient, revisited) Using our newfound knowledge about μ, prove the formula for ϕ.

(b) **[2]** Write down a non-recursive formula for Φ_n.

(c) **[2]** Show that the primitive n-th roots of unity sum to $\mu(n)$. (This is quite useful for an earlier problem, but I'm not telling you which!)

Solution to Problem 34:

(a)
$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d} = n\sum_{d|n}\mu(d)$$

(b)
$$\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu[n/d]}$$

(c) If s_n were the sum of the primitive n-th roots of unity, then $\sum_{d|n} s_n = 0$ unless $n = 1$, then the sum is 1.

35. For this problem, we will analyze cyclotomic coefficients and deduce some nontrivial facts about the coefficient of $\Phi_n(x)$ given some control over n.

(a) **[5]** Consider cyclotomic polynomials of the form $\Phi_{pq}(x)$ where p and q are distinct primes. Demonstrate that the coefficients of $\Phi_{pq}(x)$ lie within the set $\{0, \pm 1\}$. We call such a cyclotomic polynomial **flat**.

(Hint. The largest number that cannot be represented as $xp + yq$ for some $x, y \in \mathbb{N}$ is exactly $\phi(pq) - 1$.)

(b) **[7]** Are there cyclotomic polynomials which are not flat? Justify your answer.

Solution to Problem 35:

(a) The formula gives
$$\Phi_{pq}(x) \equiv \frac{(1-x)}{(x^p-1)(x^q-1)} \pmod{x^{pq}}$$

However, $[(x^p - 1)(x^q - 1)]^{-1} \pmod{x^{pq}}$ only has coefficients in $\{0, 1\}$, so the claim follows.

(b) There are many answers, but $\Phi_{7\cdot11\cdot13}(x)$ is not flat. Suppose p, q, r are prime numbers such that $p < q < r < 2p$. Then,
$$\begin{aligned}\Phi_{pqr}(x) &\equiv (x^p-1)(x^q-1)(x^r-1)\cdot(x-1)^{-1} \pmod{x^{2p}} \\ &\equiv (1-x^p-x^q-x^r)(1+x+x^2+\cdots) \pmod{x^{2p}}\end{aligned}$$

Thus it is clear that the coefficient of x^r is -2.

3.5 Cyclotomy and Primes

The structure of cyclotomic polynomials gives us interesting consequences about the primes that divide $a^n - 1$.

36. This problem concerns special cases of the Dirichlet's Theorem on Arithmetic Progressions, which states that for any coprimes $k.n$, there are infinitely many primes which are $k \pmod n$. We will only be able to show this for $k = 1$.

    (a) **[1]** Here's a familiar case. Prove that if p is a prime and x is an integer, then if $p \mid x^2 + 1$ then $p \equiv 1 \pmod 4$. As a consequence, show that there are infinitely many primes that are $\equiv 1 \pmod 4$.

    (b) **[5]** Show that for every positive integer n and integer $a > 1$, any prime factor of $\Phi_n(a)$ is either $1 \pmod n$ or divides n. Conclude that there are infinitely many primes that are $\equiv 1 \pmod n$.

    Solution to Problem 36:

    (a) This is just the quadratic residue criterion for p. (see the first section).

    (b) We will cheat a little and use D.2(c): that gives $\gcd(\Phi_n(a), a^d - 1)$ divides n for any proper factor $d \mid n, d < n$. So for a prime factor of $\Phi_n(a)$ not dividing n, n is the order of $a \pmod p$, and so $n \mid p - 1$.

    The proof then proceeds as follows: suppose $p_1, \cdots, p_k$ are the only primes that are $1 \pmod n$. Then consider $\Phi_n(a)$ for $a = np_1 \cdots p_k$. Any prime factor $q \mid \Phi_n(a)$ is clearly coprime to a because $\Phi_n(0) = 1$, so it can't divide n, so it is $1 \pmod n$. But it can't be one of our earlier primes, since it is coprime to them all.

37. Here is an even better version of the above. For this problem, we will prove the following theorem:

    Theorem. (ineffective Zsigmondy) For all $a \geq 2021$, $n \geq 3$, there exists a prime factor of $a^n - 1$ which does not divide $a^m - 1$ for any $m < n$.

    (a) **[2]** Show that this theorem implies that there are infinitely many primes which are $1 \pmod n$ for $n \geq 3$.

    (b) **[1]** Here's a baby version of what we want to prove. Show that there exists a prime factor dividing $2^{2^n} - 1$ that does not divide $2^{2^m} - 1$ for $m < n$.

    (c) **[2]** Now we dive right in. Show that for any integer a, and d a factor of m, $\gcd(\Phi_m(a), a^d - 1)$ divides $\Phi_{m/d}(1)$.

    (d) **[4]** Show that $p \mid \Phi_n(a)$ implies that n/d is a power of p, and $p^2 \mid \Phi_n(a)$ implies $n = d$. Consequently, prove the following lemma:

    Lemma. The following holds for positive integers $m < n$:

    (i) $\gcd(\Phi_m(a), \Phi_n(a)) > 1$ only when n/m is a prime power of some prime p.

    (ii) Even if n/m is a prime power of p, p^2 does not divide $\Phi_n(a)$ (so the gcd is 1 or p).

    (You may use this fact about "orders" without proof: if d is the minimal positive integer such that $p \mid a^d - 1$, then $p \mid a^n - 1$ if and only if $d \mid n$.)

(e) **[5]** Prove the ineffective version of Zsigmondy's theorem given at the start of this section: for all $a \geq 2021$, $n \geq 3$, there exists a prime factor of $a^n - 1$ which does not divide $a^m - 1$ for any $m < n$.

(f) **[2]** You may suspect that the assumed size conditions on a, n are somewhat "loose". This can be improved to obtain almost all pairs of integers (a, n), with the following exceptions:

- $a = 1$, because then $a^n - 1 = 0$ and that's bad.
- $n = 1, a = 2$, because then $a^n - 1 = 1$ and it has no prime divisors
- An infinite family of (a, n) with fixed n.
- A lone case (a, n).

What exactly are the last two cases above? (We do not require a proof that these are the only cases, just that these are counterexamples.) In fact, the full version of Zsigmondy's theorem tells us that these are the only counterexamples.

Solution to Problem 37:

(a) Suppose otherwise, then let $p_1, \cdots, p_k$ be all the primes which are 1 (mod n). Let $\Pi = p_1 p_2 \cdots p_k$ be the product of all these primes. Then, pick large enough m such that $\Pi^m > 2021$, then $\Pi^{mn} - 1$ has a prime factor q that doesn't divide any $\{\Pi^\ell - 1\}_{\ell < mn}$, so the order of Π (mod q) is mn, hence $n \mid q - 1$. So q is a prime that is 1 (mod n) and obviously distinct from all our previous primes (since Π is coprime with q).

(b) Since $2^{2^n} - 1 = (2^{2^{n-1}} - 1)(2^{2^{n-1}} + 1)$, just pick a prime factor of $2^{2^{n-1}} + 1$.

(c) Recall the identity

$$\Phi_n(x^k) = \prod_{d \mid k} \Phi_{dk}(x)$$

so $\Phi_m(a) \mid \Phi_{m/d}(a^d)$, hence the conclusion follows.

(d) $\gcd(\Phi_n(a) - 1, a^d - 1)$ divides $\Phi_{n/d}(1)$, and p divides that iff n/d is a prime power of p.

If $p \mid \Phi_m(a), \Phi_n(a)$, then both $m/d, n/d$ are powers of p, so n/m is a power pf p. If n/m is a power of p, then this gcd divides $\gcd(\Phi_n(a) - 1, a^m - 1)$, which divides $\Phi_{n/m}(1)$.

(e) It is sufficient to show that $\Phi_n(a)$ has a prime factor not dividing any $\Phi_m(a)$ for all $m < n$. Suppose otherwise.

If $p \mid \Phi_n(a)$, then if n is the order of p, we're done. Otherwise, p divides n and $p^2 \nmid \Phi_n(a)$, so $\Phi_n(a) \mid n$. But,

$$\Phi_n(a) = \prod_{(k,n)=1, k<n} \left| a - \zeta_n^k \right| \geq (a-1)^{\phi(n)} > n$$

by a fast and loose bound: $\phi(n) \geq \sqrt{2n}$, and $2^{\sqrt{2n}} > n$ for $n \geq 10$, while $n < 10$ is trivial to check because a is assumed to be large.

(f) $(2^k - 1, 2)$ and $(2, 6)$.