UBC Math Circle 2021 Problem Set 1

1. (a) Let p be a prime number. Show that $\Phi_p(x) = \frac{x^p-1}{x-1} \in \mathbb{Z}[x]$ is irreducible.

> **Solution:** Note $\Phi_p(x) \in \mathbb{Z}[x]$ is irreducible if and only if $\Phi_p(x+1) \in \mathbb{Z}[x]$ is irreducible. Compute $\Phi_p(x+1) = \frac{(x+1)^p-1}{x} = \sum_{i=0}^{p-1} \binom{p}{i+1} x^k$, which is irreducible in $\mathbb{Z}[x]$ by Eisenstein's criterion.

(b) Show that $\Phi_{p^r}(x) = \frac{x^{p^r}-1}{x^{p^{r-1}}-1} \in \mathbb{Z}[x]$ is irreducible for any $r \in \mathbb{N}$.

> **Solution:** We will show that $\Phi_{p^r}(x+1)$ is Eisenstein. To see this, note that $(x+1)^{p^r}-1$ and $(x+1)^{p^{r-1}}-1$ are equivalent to $(x+1-1)^{p^r}$ and $(x+1-1)^{p^{r-1}}$, respectively, modulo p. (Apply induction on the relation $(f-g)^p \equiv f^p - g^p \bmod p$.)
> Therefore, $\Phi_{p^r}(x+1)$ is equivalent to $x^{p^r-p^{r-1}}$ modulo p. Moreover, the constant term of $\Phi_{p^r}(x+1)$ is $\Phi_{p^r}(1) = \sum_{i=0}^{p-1} 1^{p^{r-1}i} = p$.
> So $\Phi_{p^r}(x+1)$ is Eisenstein and so Φ_{p^r} is irreducible.

2. Show for $n \geq 5$ that $1 + \prod_{i=1}^{n}(x-i) \in \mathbb{Z}[x]$ is irreducible.

> **Solution:** If the polynomial were reducible in $\mathbb{Z}[x]$, there would exist $f, g \in \mathbb{Z}[x]$ both of degree $< n$ such that $fg = 1 + \prod_{i=1}^{n}(x-i)$. Then since $f(i)g(i) = 1$ for each $1 \leq i \leq n$, it follows that $f(i) = g(i)$ for each $1 \leq i \leq n$ (as they are either both -1 or both 1). Then $f - g \in \mathbb{Z}[x]$ is a polynomial of degree $< n$ but has at least n distinct roots, so $f - g$ must be the zero polynomial.
>
> It remains to check that $1 + \prod_{i=1}^{n}(x-i)$ cannot be written as f^2 for some $f \in \mathbb{Z}[x]$. It is clearly not possible for odd n. For even $n \geq 6$, evaluating the polynomial at 1.5 gives a negative value, so the polynomial cannot be square.

3. Show that $x^4 + 1$ is irreducible in $\mathbb{Z}[x]$ but not in $\mathbb{Z}/p\mathbb{Z}[x]$ for any prime p.

> **Solution:** Clearly $x^4 + 1$ has no roots in $\mathbb{Q}$, so $x^4 + 1$ cannot be factored as the product of a degree 1 polynomial and a degree 3 polynomial in $\mathbb{Z}[x]$. If $x^4 + 1$ can be factored as the product of two quadratics in $\mathbb{Z}[x]$, then it can be written as $(x^2 + ax \pm 1)(x^2 - ax \pm 1) = x^4 + (\pm 2 - a^2)x^2 + 1$ for some $a \in \mathbb{Z}$. This is not possible, because $a^2 = \pm 2$ has no solutions in $\mathbb{Z}$.
>
> In $\mathbb{Z}/2\mathbb{Z}[x]$, the polynomial $x^4 + 1$ has 1 as a root since $1^4 + 1 \equiv 0 \bmod 2$, and so has $x - 1$ as a factor.

For odd p, if -1 is square in $\mathbb{Z}/p\mathbb{Z}$, then x^4+1 is a difference of squares, and so would be reducible. Additionally, if one of ± 2 is square in $\mathbb{Z}/p\mathbb{Z}$, then x^4+1 can be written as a product in the form $(x^2+ax\pm 1)(x^2-ax\pm 1)$. So it suffices to show that least one of $-1, \pm 2$ is square in $\mathbb{Z}/p\mathbb{Z}$. Let g be a primitive root modulo p. If -1 and 2 are both not square in $\mathbb{Z}/p\mathbb{Z}$, then they can be written as powers of g with odd exponent. Then their product -2 can be written as a power of g with even exponent, and so is square in $\mathbb{Z}/p\mathbb{Z}$.

4. (a) Show that for a prime $p \equiv 3 \pmod 4$, $x^2+y^2 \equiv 0 \pmod p$ implies $x \equiv y \equiv 0 \pmod p$

Solution: Suppose that $x, y \not\equiv 0 \pmod p$ (if, say, $x \equiv 0 \pmod p$ then $y \equiv 0 \pmod p$). From $x^2 \equiv -y^2 \pmod p$ we have $(x^2)^{(p-1)/2} \equiv (-y^2)^{(p-1)/2} \pmod p$, hence $x^{p-1} \equiv -y^{p-1}$ (note that $\frac{p-1}{2}$ is odd). Hence $1 \equiv -1 \pmod p$ by Fermat's little theorem, which is a contradiction.

(b) Find the solutions to the following congruence:

$$2x^2+6xy-2x+5y^2-4y+1 \equiv 0 \pmod{2021}$$

Solution: Note that

$$2x^2+6xy-2x+5y^2-4y+1 = (x+y)^2+(x+2y-1)^2$$

and since we have the factorization into primes $2021 = 43 \cdot 47$ where $43 \equiv 47 \equiv 3 \pmod 4$, from the congruence equation we must have

$$x+y \equiv x+2y-1 \equiv 0 \pmod{43}$$
$$x+y \equiv x+2y-1 \equiv 0 \pmod{47}$$

by part (a). Hence we have $x \equiv -1 \pmod{43}, y \equiv 1 \pmod{43}$ and $x \equiv -1 \pmod{47}, y \equiv 1 \pmod{47}$.
Which gives the solution $x \equiv -1 \pmod{2021}$ and $y \equiv 1 \pmod{2021}$.

5. (QM-AM-GM-HM inequality) Let $x_1, \ldots, x_n$ be n positive real numbers. Then

$$\sqrt{\frac{x_1^2+\cdots+x_n^2}{n}} \geq \frac{x_1+\cdots+x_n}{n} \geq \sqrt[n]{x_1 \cdot \cdots \cdot x_n} \geq \frac{n}{\frac{1}{x_1}+\cdots+\frac{1}{x_n}}.$$

Solution: https://artofproblemsolving.com/wiki/index.php/Root-Mean_Square-Arithmetic-Mean-Geometric_Mean-Harmonic_mean_Inequality

6. Let a, b, c be positive real numbers. Show that

$$\frac{1}{2a} + \frac{1}{2b} + \frac{1}{2c} \geq \frac{1}{a+b} + \frac{1}{b+c} + \frac{1}{c+a}.$$

Solution: Using the AM-GM-HM inequality, we have

$$\frac{2}{a+b} = \frac{2}{\frac{1}{a^{-1}} + \frac{1}{b^{-1}}} \leq \frac{a^{-1} + b^{-1}}{2}.$$

Using the above inequality on each of the terms on the right hand side, we get

$$\begin{aligned}
\frac{1}{a+b} + \frac{1}{b+c} + \frac{1}{c+a} &= \frac{1}{2}\left(\frac{2}{a+b} + \frac{2}{b+c} + \frac{2}{c+a}\right) \\
&\leq \frac{1}{2}\left(\frac{a^{-1}+b^{-1}}{2} + \frac{b^{-1}+c^{-1}}{2} + \frac{c^{-1}+a^{-1}}{2}\right) \\
&= \frac{1}{2}\left(a^{-1} + b^{-1} + c^{-1}\right) \\
&= \frac{1}{2a} + \frac{1}{2b} + \frac{1}{2c}.
\end{aligned}$$

7. Let x, y, z be positive reals satisfying $x^2 + y^2 + z^2 = 2xy + 2xz + 2yz$. Prove that

$$\frac{x+y+z}{3} \geq \sqrt[3]{2xyz}.$$

Solution: Write $x + y + z = \frac{x+y-z}{2} + \frac{x+y-z}{2} + 2z$, and apply AM-GM to obtain $\frac{x+y+z}{3} \geq \sqrt[3]{2xyz}$, noting that the given equation tells us $(x + y - z)^2 = 4yz$.

Parametrizing (assuming without loss of generality $z \geq x, y$) $x = a^2$, $y = b^2$, giving $z = (a + b)^2$, as suggested during the discussion, will also work.

8. Let $n \geq 2$ be an integer. Prove that

$$n\left(1 - \frac{1}{\sqrt[n]{n}}\right) + 1 > 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} > n(\sqrt[n]{n+1} - 1).$$

Solution: We can rearrange the first inequality to see that it's equivalent to

$$1 - \frac{\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}}{n} > \frac{1}{\sqrt[n]{n}}.$$

Then, the AM-GM inequality gives

$$1 - \frac{\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}}{n} = \frac{1 + \frac{1}{2} + \frac{2}{3} + \cdots + \frac{n-1}{n}}{n} > \sqrt[n]{\frac{1}{n}}$$

because the product telescopes to $\frac{1}{n}$.

We can rearrange the second inequality to see that it's equivalent to

$$1 + \frac{1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}}{n} > \sqrt[n]{n+1}.$$

Then, the AM-GM inequality gives

$$1 + \frac{1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}}{n} = \frac{\frac{2}{1} + \frac{3}{2} + \frac{4}{3} + \cdots + \frac{n+1}{n}}{n} > \sqrt[n]{n+1}$$

because the product telescopes to $n+1$.

9. (Complementary Beatty sequences) Let α and β be positive irrational numbers such that $1/\alpha + 1/\beta = 1$. Show that the sequences $a_n = \lfloor \alpha n \rfloor$ and $b_n = \lfloor \beta n \rfloor$ are disjoint and their union is $\mathbb{N}$.

Solution: Step 1: We prove by contradiction that there does not exist $m, n \in \mathbb{N}$ such that $\lfloor \alpha m \rfloor = \lfloor \beta n \rfloor$. Suppose that $\lfloor \alpha m \rfloor = \lfloor \beta n \rfloor = q$ for some integer q. Then,

$$q < \alpha m < q + 1 \quad \text{and} \quad q < \beta n < q + 1.$$

The inequalities are strict because α and β are irrational. Rearranging (dividing by q and $q+1$) the above inequalities gives

$$\frac{m}{q+1} < \frac{1}{\alpha} < \frac{m}{q} \quad \text{and} \quad \frac{n}{q+1} < \frac{1}{\beta} < \frac{n}{q}.$$

Adding these two inequalities and using $1/\alpha + 1/\beta = 1$ gives

$$\frac{m+n}{q+1} < 1 < \frac{m+n}{q} \implies q < m + n < q + 1.$$

This is a contradiction because $m+n$ is an integer between two consecutive integers.

Step 2: We prove that the union of the sequences is $\mathbb{N}$. First, we show that 1 must be in one of the sequences. Note that $\alpha, \beta > 1$ because otherwise, $1/\alpha + 1/\beta > 1$. Furthermore, we cannot have both $\alpha > 2$ and $\beta > 2$ because then $1/\alpha + 1/\beta < 1$. This means that one of α or β is in $(1, 2)$, so either $\lfloor \alpha \rfloor = 1$ or $\lfloor \beta \rfloor = 1$. Now, suppose (for contradiction) that some integer $q \geq 2$ is not in either sequence. Then, we can find $m, n \in$ such that

$$\alpha m < q < q + 1 < \alpha(m + 1) \quad \text{and} \quad \beta n < q < q + 1 < \beta(n + 1).$$

Then,

$$\frac{m}{q} < \frac{1}{\alpha} < \frac{m+1}{q+1} \quad \text{and} \quad \frac{n}{q} < \frac{1}{\beta} < \frac{n+1}{q+1}.$$

Adding these two inequalities gives

$$\frac{m+n}{q} < 1 < \frac{m+n+2}{q+1} \implies m + n < q < q + 1 < m + n + 2.$$

This is a contradiction because $m + n$, q, $q + 1$, and $m + n + 2$ are all integers.