Assignment 1

Numbers Made Dumber — Abhishek Shree
Project #13 — Roll: 200028

---

1. Prove that $\frac{21n+4}{14n+3}$ is irreducible for every natural n.

Sol. For the fraction to be irreducible, $gcd(21n+4, 14n+3) = 1$, or the numerator and denominator are **coprimes**.

Lemma. This follows directly from Euclidean Algorithm,

$$\gcd(a, b) = \gcd(a-b, b) \text{ where } a > b \text{ (say)}$$

Proof.

$$\begin{aligned}
\gcd(21n+4, 14n+3) &= \gcd(7n+1, 14n+3) \\
&= \gcd(14n+3, 7n+1) \qquad \text{as } 14n+3 > 7n+1 \ \forall\, n \in \mathbb{N} \\
&= \gcd(7n+2, 7n+1) \\
&= \gcd(1, 7n+1) \\
&= 1
\end{aligned}$$

□

---

2. Find all integers n such that n^2+2n+2 divides $n^3+4n^2+4n-14$.

Sol. Upon factorisation, we get

$$n^3+4n^2+4n-14 = (n^2+2n+2)(n+2) - (2n+18)$$

Here, the quotient is $(n+2)$ and the remainder is $(-2n-18)$.
If, $-2n-18$ is not a remainder, i.e. the two polynomials are **divisible**, it should contradict Theorem 1.2.1 (from the notes), i.e. n lies in the range

$$\begin{aligned}
&|-2n-18| \geq \left|n^2+2n+2\right| \text{ or } \left|\frac{2n+18}{n^2+2n+2}\right| \geq 1 \\
\implies &\frac{2n+18}{n^2+2n+2} \geq 1 \text{ or } \frac{2n+18}{n^2+2n+2} \leq -1 \\
\implies &n^2 \leq 16 \text{ or } n^2+4n+20 \leq 0 \\
\implies &n \in [-4, 4]
\end{aligned}$$

There is also a possibilty that $-2n - 18 = 0 \implies n = -9$

All the acceptable values of n are $\boxed{\text{\{-9, -4, -2, -1, 0, 1, 4\}}}$ as other values in the range violate the condition $r \geq b$ (easy to see for $n \geq 0$, say 2 or 3).

---

3. For natural numbers a, n, m prove that $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$.

Sol. Let $b = \gcd(a^m - 1, a^n - 1)$

$\therefore a^m = 1 + kb$ and $a^n = 1 + jb$ for some j and k

Also, $gcd(m, n) = mx + ny$ by Bezout's identity. So,

$$\begin{aligned} a^{\gcd(m,n)} - 1 &= a^{mx+ny} - 1 \\ &= a^{mx}a^{ny} - 1 \\ &= (1 + kb)^x(1 + jb)^y - 1 \\ &= (\qquad \dots \qquad)b \end{aligned}$$

Hence, b divides $a^{\gcd(m,n)} - 1$. We also know that both m and n are divisible by $\gcd(m, n)$, say $m = \gcd(m, n)c$ then

$a^m - 1 = a^{\gcd(m,n)c} - 1^c \implies a^m - 1 = (a^{\gcd(m,n)} - 1)(\qquad \dots \qquad)$, where ... is some constant.

Hence, $\underline{(a^{\gcd(m,n)} - 1) \text{ divides } a^m - 1}$, similarly $a^n - 1$.

$(a^{\gcd(m,n)} - 1)$ divides both $a^m - 1$ and $a^n - 1$, therefore it must divide their gcd, i.e. b.

As, b divides $a^{\gcd(m,n)} - 1$ and $a^{\gcd(m,n)} - 1$ divides b, this implies they both are equal.

$$b = a^{\gcd(m,n)} - 1$$

OR

$$\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1 \qquad \text{Proved!}$$

---

4. Let the integers a_n and b_n be defined by the relationship

$$a_n + b_n\sqrt{2} = (1 + \sqrt{2})^n$$

for all integers $n \geq 1$. Prove that $\gcd(a_n, b_n) = 1$ for all integers $n \geq 1$.

Sol. By the Principle of Mathematical Induction,

For $n = 1$: $a_1 = 1$ and $b_1 = 1$ $\qquad \therefore \gcd(a_1, b_1) = 1$

Let $a_k + b_k\sqrt{2} = (1 + \sqrt{2})^k$ such that $\gcd(a_k, b_k) = 1$ be true for $n = k$.

For $n = k+1$:

$$\begin{aligned}
a_{k+1} + b_{k+1}\sqrt{2} &= (1+\sqrt{2})^{k+1} \\
&= (1+\sqrt{2})(1+\sqrt{2})^{k} \\
&= (1+\sqrt{2})(a_k + b_k\sqrt{2}) \\
&= (a_k + 2b_k) + (a_k + b_k)\sqrt{2} && \text{(upon rearranging)}
\end{aligned}$$

Upon comparing RHS and LHS we get,

$$a_{k+1} = a_k + 2b_k \text{ and } b_{k+1} = a_k + b_k$$

Now,

$$\begin{aligned}
\gcd(a_{k+1}, b_{k+1}) &= \gcd(a_k + 2b_k, a_k + b_k) \\
&= \gcd(b_k, a_k + b_k) \\
&= \gcd(b_k, a_k) && \text{(as assumed above)} \\
&= 1
\end{aligned}$$

Hence the relation holds for $n = k+1$ given $n = k$.

Therefore, we conclude that relationship hold for all integers $n \geq 1$.

---

5. If p is an odd prime, and a, b are relatively prime positive integers, prove that

$$\gcd\left(a+b, \frac{a^p + b^p}{a+b}\right) = 1 \text{ or } p.$$

Sol.

Here,

$$\boxed{\frac{a^p + b^p}{a+b} = a^{p-1}b^0 - a^{p-2}b^1 + \ldots - a^1b^{p-2} + a^0b^{p-1}} \qquad (A)$$

On dividing $\frac{a^p+b^p}{a+b}$ by $a+b$ we get,

$$a^{p-1}b^0 - a^{p-2}b^1 + \ldots - a^1b^{p-2} + a^0b^{p-1} = (a+b)(a^{p-2} - 2a^{p-3}b^1 + \ldots) + pb^{p-1}$$

The remainder $= pb^{p-1}$, but if we reverse the RHS in (A) and then divide we end up getting

$$b^{p-1}a^0 - b^{p-2}a^1 + \ldots - b^1a^{p-2} + b^0a^{p-1} = (a+b)(b^{p-2} - 2b^{p-3}a^1 + \ldots) + pa^{p-1}$$

So if we assume that $d = \gcd\left(a+b, \frac{a^p+b^p}{a+b}\right)$, then d must divide both pb^{p-1} and pa^{p-1}.

As $\gcd(a,b) = 1 \implies \gcd(a^{p-1}, b^{p-1}) = 1$

As a^p and b^p are coprimes, d needs to either be 1 or p to divide both pa^{p-1} and pb^{p-1} simultaneously.

Hence, $\gcd\left(a+b, \frac{a^p+b^p}{a+b}\right) = 1$ or p

---

6. If $a|bc$ and $\gcd(a,b) = 1$, prove that $a|c$.

Sol. Constructing a Linear Diophantine Equation, $ax + by = 1$, which also means that

$$cax + cby = c$$

We are given that a divides bc, a also divides ac (trivial).

Let $bc = ap$ for some p. The equation converts to, $cax + apy = c$ or $a(cx + py) = c$ where $(cx + py) \in \mathbb{Z}$.

Hence, a divides c.

---

7. Prove that the expression

$$\frac{\gcd(m,n)}{n}\binom{n}{m}$$

is an integer for all pairs of integer $n \geq m \geq 1$.

Sol. Let $\gcd(m,n) = mx + ny$ for some integers x, y.

$$\begin{aligned}\frac{\gcd(m,n)}{n}\binom{n}{m} &= \frac{(mx+ny)}{n}\binom{n}{m} \\ &= \frac{xm}{n}\binom{n}{m} + y\binom{n}{m} \\ &= x\binom{n-1}{m-1} + y\binom{n}{m} \in \mathbb{Z} \qquad \textit{Proved.}\end{aligned}$$

---

8. Let $n, p > 1$ be positive integers and p be a prime. Given that $n|p-1$ and $p|n^3-1$, prove that $4p-3$ is a perfect square.

Sol. As n divides $(p-1)$ and p divides (n^3-1), we can write $(p-1) = nx \implies p = (nx+1)$ and $(n^3-1) = py$ for x and $y \in \mathbb{Z}$.

Also $(n^3-1) = (n-1)(n^2+n+1)$, but as $p = nx+1$ it implies that $p \geq n+1$, hence p cannot divide $n-1(< p) \implies$ it is the (n^2+n+1) term that is divisible by p.

$$\therefore\ n^2+n+1 \geq p \tag{1}$$

$$\geq nx+1 \implies \boxed{x \leq n+1}$$

if $x < n+1$, then $nx+1 = p < n(n+1)+1 = n^2+n+1$ which cannot be true as p divides n^2+n+1 (violates inequality 1).

$\therefore x = n+1$ is the only acceptable solution here. Putting $x = n+1$ in p we get,

$$p = nx+1 = n(n+1)+1 = n^2+n+1$$

$$\begin{aligned}\therefore 4p-3 &= 4(n^2+n+1)-3 \\ &= (2n+1)^2 \qquad \text{which is a perfect square.}\end{aligned}$$

---

9. Find all pairs of positive integers a, b such that

$$\frac{a^2+b}{b^2-a} \text{ and } \frac{b^2+a}{a^2-b}$$

are both integers.

Sol. If such integers exist, then

$$(a^2+b) \geq (b^2-a) \text{ and } (b^2+a) \geq (a^2-b)$$

$$(a+b)(a-b+1) \geq 0 \text{ and } (a+b)(b-a+1) \geq 0$$

$$\implies \boxed{a \geq b-1 \text{ and } b \geq a-1}$$

This inequality holds only when $a = b$ or $a = b-1$ or $a = b+1$.

For any other a, say $a = b+k; k > 1$ or $k < -1$ it will satisfy only one of the two inequalities. Hence, no other solutions are possible.

Case 1: If $a = b$, then

$$\frac{a^2+b}{b^2-a} = \frac{b^2+a}{a^2-b} = \frac{a^2+a}{a^2-a} = \frac{a+1}{a-1} = 1 + \frac{2}{a-1} \in \mathbb{Z}$$

Therefore $a = 2$ or $a = 3$ are the only solution here.

Case 2: If $a = b - 1$,

$$\frac{b^2+a}{a^2-b} = \frac{b^2+b-1}{(b-1)^2-b} = \frac{b^2+b-1}{b^2-3b+1} = 1 + \frac{4b-2}{b^2-3b+1}$$

For this expression to be an integer,

$$4b - 2 \geq b^2 - 3b + 1 \implies b^2 - 7b + 3 \leq 0 \implies b \in \{1, 2, 3, 4, 5, 6\}$$

If $b = 1$,then $a = 0 \notin \mathbb{Z}^+$. Hence, $b = 1$ is not a solution. $b = \{4, 5, 6\}$ does not make the whole term ineger. So the only possible solutions here are $b = \{2, 3\}$

Case 3: If $a = b + 1$,

$$\frac{a^2+b}{b^2-a} = \frac{a^2+a-1}{(a-1)^2-a} = \frac{a^2+a-1}{a^2-3a+1} = 1 + \frac{4a-2}{a^2-3a+1}$$

For this expression to be an integer,

$$4a - 2 \geq a^2 - 3a + 1 \implies a^2 - 7a + 3 \leq 0 \implies a \in \{1, 2, 3, 4, 5, 6\}$$

If $a = 1$,then $b = 0 \notin \mathbb{Z}^+$. Hence, $a = 1$ is not a solution. $a = \{4, 5, 6\}$ does not make the whole term ineger. So the only possible solutions here are $a = \{2, 3\}$

Hence the total possible $(a, b) = \{(2, 2), (3, 3), (1, 2), (2, 1), (2, 3), (3, 2)\}$

---

10. For $m > 1$, it can be proven that the integer sequence $f_m(n) = \gcd(n + m, mn + 1)$ has a fundamental period T_m. In other words,

$$\forall\, n \in \mathbb{N}, f_m(n + T_m) = f_m(n)$$

Find an expression for T_m in terms of m.

Sol. By applying the Euclidean Algorithm, we get

$$\begin{aligned} f_m(n) &= \gcd(n + m, mn + 1) \\ &= \gcd(n + m, m(m + n) - m^2 + 1) \\ &= \gcd(n + m, -m^2 + 1) && \because \gcd(a, b) = \gcd(a, b + at) \end{aligned}$$

This expression $f_m(n) = \gcd(n + m, 1 - m^2)$ is nice. To show f is periodic we can use this. Let $f_m(n + x) = f_m(n)$ for some x, i.e.

$$\gcd(m + n + x, 1 - m^2) = \gcd(m + n, 1 - m^2) \implies x = (1 - m^2)k$$

$\therefore$ The fundamental period of the function is $\boxed{T_m = |1 - m^2|}$.