

Selected Solutions

Web Problem #2: Let

$$C_r^n = \frac{n!}{r! \cdot (n-r)!}.$$

Show that C_r^n is an integer.

Proof: From class, we know that the number of times the prime p appears in the factorization of $n!$ is given by

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots.$$

Similarly, the number of times the prime p appears appears in the factorization of $r! \cdot (n-r)!$ is given by

$$\left\lfloor \frac{r}{p} \right\rfloor + \left\lfloor \frac{r}{p^2} \right\rfloor + \left\lfloor \frac{r}{p^3} \right\rfloor + \cdots + \left\lfloor \frac{n-r}{p} \right\rfloor + \left\lfloor \frac{n-r}{p^2} \right\rfloor + \left\lfloor \frac{n-r}{p^3} \right\rfloor + \cdots.$$

In order for C_r^n to be an integer, for any p there must be at least as many factors of p in the numerator than in the denominator. In other words, the first expression must be greater than or equal to the bottom expression. Therefore, it is enough to prove that

$$\left\lfloor \frac{n}{p^k} \right\rfloor \geq \left\lfloor \frac{r}{p^k} \right\rfloor + \left\lfloor \frac{n-r}{p^k} \right\rfloor.$$

This result would follow if we can prove that

$$\lfloor x + y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor.$$

Any real number z can be written as $z = \lfloor z \rfloor + \{z\}$ where $\{z\}$ is called the *fractional part of z* and satisfies $0 \leq \{z\} < 1$.

We will use the following property of the greatest integer function: If n is an integer, then

$$\lfloor n + z \rfloor = n + \lfloor z \rfloor.$$

(Try to prove this! Hint: $\lfloor z \rfloor$ is defined to be the *unique* integer satisfying $\lfloor z \rfloor \leq z < \lfloor z \rfloor + 1$.)

So we have

$$\begin{aligned} \lfloor x + y \rfloor &= \lfloor \lfloor x \rfloor + \{x\} + \lfloor y \rfloor + \{y\} \rfloor \\ &= \lfloor x \rfloor + \lfloor y \rfloor + \lfloor \{x\} + \{y\} \rfloor, \text{ since } \lfloor x \rfloor + \lfloor y \rfloor \text{ is an integer} \\ &\geq \lfloor x \rfloor + \lfloor y \rfloor, \text{ since } 0 \leq \{x\} + \{y\} < 2, \text{ we have } \lfloor \{x\} + \{y\} \rfloor \geq 0. \end{aligned}$$

Comments:

- If you make claims such as $\lfloor \{x\} + \{y\} \rfloor = 0$ or 1 , then you should explain why it is true.

- There's another way to prove this, which is by showing that the product of any n consecutive integers is divisible by $n!$. For example, $8 \cdot 7 \cdot 6$ is divisible by $3!$. If you understand how you got the formula for the number of times a prime p appears in the factorization of $n!$, then you should be able to prove this claim.

Web Problem #3a: Suppose that

$$f(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_1x + a_0$$

is a polynomial with integer coefficients whose leading coefficient is 1. If α is a root of $f(x)$ and α is not an integer, show that α must be irrational.

Proof: Suppose by contradiction that $\alpha = m/n$, where m and n are relatively prime with $n \neq 0$ (that is, α is rational). Since α is a root of $f(x)$, we have

$$0 = \left(\frac{m}{n}\right)^k + a_{k-1}\left(\frac{m}{n}\right)^{k-1} + \cdots + a_1\left(\frac{m}{n}\right) + a_0.$$

Multiplying through by n^k to clear the denominators gives

$$0 = m^k + a_{k-1}m^{k-1}n + \cdots + a_1mn^{k-1} + a_0n^k.$$

From this, we can solve for m^k :

$$m^k = n(-a_{k-1}m^{k-1} - \cdots - a_1mn^{k-2} - a_0n^{k-1}).$$

This implies that $n \mid m^k$.

Suppose there is a prime p dividing n . Then since $p \mid n$ and $n \mid m^k$, we have $p \mid m^k$ (by Theorem 1.3). But then we have $p \mid m$ (by Theorem 2.8). This gives a contradiction since $p \mid n$ and $p \mid m$ implies $p \mid (n, m) = 1$.

So there are no primes p dividing n . This means $n = \pm 1$. But then $\alpha = m/n = \pm m$ is an integer, contradicting our assumption. Therefore, α cannot be rational, which is to say that α is irrational.

Comments:

- From $n \mid m^k$, you might want to conclude that $n \mid m$. However, this is false (for example, $4 \mid 6^2$). Theorem 2.8 only applies if n is a prime.
- You can prove that if $n \mid m^k$ and $(n, m) = 1$ that $n \mid m$ by repeatedly using Theorem 2.6. You should try to write up this proof for yourself.

Web Problem #4b: Show that there are infinitely many primes of the form $4k - 1$.

Proof: Suppose by contradiction that there are only finitely many primes of the form $4k - 1$. We shall label all of these primes by p_1, p_2, \dots, p_r . Consider the number $N = 4p_1p_2 \cdots p_r - 1$. Notice that N is of the form $4k - 1$ and $N > 1$.

Also notice that none of the p_i can divide N . This is true since if some p_i divided N then it would divide $N - 4p_1p_2 \cdots p_r = -1$, but no primes divide 1.

There are two cases to consider. Either N is prime or it is composite.

If N is prime, then it is a prime of the form $4k - 1$, so it must be one of the p_i . However, this is impossible since none of the p_i divide N . So N cannot be prime.

If N is composite, then it can be factored into a product of primes (Theorem 1.5). We already know that no primes of the form $4k - 1$ divide N , so this factorization can only contain primes of the form $4k + 1$ or 2. But since N is odd, we know that $2 \nmid N$. Therefore, N factors into a product of primes of the form $4k + 1$.

By problem 4a, a product of numbers of the form $4k + 1$ is also of the form $4k + 1$. This is a contradiction since N is of the form $4k - 1$. So N cannot be composite.

We have shown that N is a number larger than 1 that is neither prime or composite. This is a contradiction to Theorem 1.5, so our initial assumption must be false. Therefore, there must be infinitely many primes of the form $4k - 1$.