Putnam practice - Number theory problem solutions

1. True or false: If $p \geq 5$ is a prime number, then 24 divides $p^2 - 1$ without remainder.

True.

First note that $p^2 - 1$ can be factored as $(p-1)(p+1)$.

Observe that one of any three consecutive integers $p-1, p, p+1$ must be divisible by 3. However, since $p \geq 5$ is a prime, p cannot be divisible by 3. Hence, 3 divides one of $p-1$ or $p+1$, and their product.

Next, observe that one of any four consecutive integers $p-1, p, p+1, p+2$ must be divisible by 4. However, since $p \geq 5$ is prime, p cannot be even and, hence, $p+2$ cannot be even.

Therefore, 4 divides one of $p-1$ or $p+1$. Then the remaining one is also an even number and is divisible by 2. Hence, $4 \cdot 2 = 8$ divides $(p-1)(p+1)$.

Combining everything together, we have $3 \cdot 8 = 24$ divides $(p-1)(p+1) = p^2 - 1$.

2. Show that there are no integers a, b, and c such that $a^2 + b^2 - 8c = 6$.

The equation is the same as $a^2 + b^2 = 8c + 6$.

Now, we try to study perfect squares $x^2 \pmod 8$.

By division algorithm, any integer x has remainder $0, 1, 2, 3, 4, 5, 6$ or 7 when divided by 8. (i.e., $x \equiv 0, 1, 2, 3, 4, 5, 6, 7 \pmod 8$.)

One can verify that $x^2 \equiv 0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2 \equiv 0, 1, 4, 1, 0, 1, 4, 1 \pmod 8$.

So, any perfect square $x^2 \equiv 0, 1$ or $4 \pmod 8$.

Consequently, $a^2 + b^2 \equiv 0+0, 0+1, 0+4, 1+0, 1+1, 1+4, 4+0, 4+1$ or $4+4 \pmod 8$ but none of these is $\equiv 6 \pmod 8$.

Therefore, there is no integer solution to $a^2 + b^2 = 8c + 6$.

3. (2003 A1) Let n be a fixed positive integer. How many ways are there to write n as a sum of positive integers $n = a_1 + a_2 + \cdots + a_k$ with k positive and $a_1 \leq a_2 \leq \cdots \leq a_k \leq a_1 + 1$?

One can inspect small cases first and see a pattern.

$1 = 1$. There is only 1 way.

$2 = 2$ or $2 = 1 + 1$. There are 2 ways.

$3 = 3$, $3 = 1 + 2$, or $3 = 1 + 1 + 1$. There are 3 ways.

In general, one suspects that there are n ways to write n in the required form.

As $a_i \geq 1$, we have $n = a_1 + a_2 + \cdots + a_k \geq 1 + 1 + \cdots + 1 = k \geq 1$.

Claim: For each length $1 \leq k \leq n$, there is one and only one way to write $n = a_1 + a_2 + \cdots a_k$ with $a_1 \leq a_2 \leq \cdots \leq a_k \leq a_1 + 1$.

Proof:

Since $a_1 \leq a_2 \leq \cdots \leq a_k \leq a_1 + 1$, a certain number of the a_i's are a_1 while the rest (which could be none) are $a_1 + 1$.

Suppose $a_1 = a_2 = \cdots = a_s$ and $a_{s+1} = \cdots = a_k = a_1 + 1$ for some $1 \le s \le k$. (When $s = k$, then none of the a_i's equal to $a_1 + 1$.)

Then $n = sa_1 + (k-s)(a_1+1) = ka_1 + (k-s)$. Note that $0 \le k - s < k$.

For each length $1 \le k \le n$ of the sum $n = a_1 + a_2 + \cdots + a_k$, we know that $n = k \cdot q + r$ for some unique quotient q and remainder $0 \le r < k$ by division algorithm.

Hence, we can represent n as $n = \underbrace{q + q + \cdots + q}_{s \text{ times}} + \underbrace{(q+1) + \cdots + (q+1)}_{k-s \text{ times}}$. (i.e., there is at least one way to do it.)

Moreover, by the uniqueness of division algorithm, the equation $n = ka_1 + (k-s) = kq + r$ has only one solution for a_1 and $k - s$ (i.e., s) for each fixed k.

Therefore, the claim is true and there are exactly n ways to do it.

4. (2014 A1) Prove that every non-zero coefficient of the Taylor series of $(1 - x + x^2)e^x$ about $x = 0$ is a rational number whose numerator (in lowest terms) is either 1 or a prime number.

Recall the Taylor series for $e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$.

Then the Taylor series for $(1 - x + x^2)e^x = e^x - xe^x + x^2e^x$ is

$$\sum_{n=0}^{\infty} \frac{x^n}{n!} - \sum_{m=0}^{\infty} \frac{x^{m+1}}{m!} + \sum_{k=0}^{\infty} \frac{x^{k+2}}{k!} = \sum_{n=0}^{\infty} \frac{x^n}{n!} - \sum_{n=1}^{\infty} \frac{x^n}{(n-1)!} + \sum_{n=2}^{\infty} \frac{x^n}{(n-2)!}$$

$$= 1 + \frac{x}{1!} - \frac{x}{0!} + \sum_{n=2}^{\infty} \Big(\frac{1}{n!} - \frac{1}{(n-1)!} + \frac{1}{(n-2)!} \Big) x^n = 1 + 0x + \sum_{n=2}^{\infty} \frac{n(n-1) - n + 1}{n!} x^n$$

$$= 1 + \sum_{n=2}^{\infty} \frac{(n-1)^2}{n!} x^n = \frac{1}{1} + \sum_{n=2}^{\infty} \frac{n-1}{n \cdot (n-2)!} x^n$$

after re-indexing and some algebra. Clearly, the constant term has numerator 1.

Case 1: If $n - 1$ is a prime number, then the coefficient $\frac{n-1}{n \cdot (n-2)!}$ is in lowest term already as $n - 1$ is not divisible by $n - 2, n - 3, \ldots, 2$; and $\gcd(n-1, n) = 1$ since any common divisor of $n - 1$ and n must divide their difference which is 1. In this case, the numerator $n - 1$ is a prime number.

Case 2: If $n - 1$ is a composite number, then $n - 1 = a \cdot b$ for some $1 < a, b < n - 1$.

Subcase 1: If $a \ne b$, say $1 < a < b < n - 1$. Then both a and b appears somewhere in $(n-2)! = (n-2) \cdots b \cdots a \cdots 1$. So, the coefficient $\frac{n-1}{n \cdot (n-2)!} = \frac{ab}{n \cdot (n-2) \cdots b \cdots a \cdots 1}$ can be reduced to $\frac{1}{n \cdot \cdots}$ which has numerator 1.

Subcase 2: If $a = b$, then $n - 1 = a^2$. Then the coefficient $\frac{n-1}{n \cdot (n-2)!} = \frac{a^2}{n \cdot (n-2) \cdots 2a \cdots a \cdots 1}$ can be reduced to $\frac{1}{n \cdot \cdots}$ which has numerator 1 if $2a \le n - 2 = a^2 - 1$.

We know that $(a-1)^2 \ge 2^2 \ge 2$ when $a \ge 3$. Hence, $a^2 - 2a + 1 \ge 2$ which implies $a^2 - 1 \ge 2a$. Thus, subcase 2 above is okay when $a \ge 3$.

It remains to deal with the special case when $a = 2$. Then $n - 1 = 2^2$ gives $n = 5$. The coefficient for x^5 is $\frac{5-1}{5 \cdot (5-2)!} = \frac{4}{5 \cdot 3 \cdot 2 \cdot 1} = \frac{2}{15}$ whose numerator 2 is a prime number. And we are okay in this situation as well.

5. (2005 A1) Show that every positive integer is a sum of one or more numbers of the form $2^r 3^s$ where r and s are non-negative integers and no summand divides another.

For any positive even integer n, we can factor out the highest power of 2 that goes into it, say 2^k. Then $\frac{n}{2^k} = m$ is a positive odd integer.

Now, if we can represent m as a sum of one or more numbers of the form $2^r 3^s$ where r and s are non-negative integers and no summand divides another, then we can represent n as a sum of one or more numbers of the form $2^{r+k}3^s$ where r and s are non-negative integers and no summand divides another.

Therefore, we can focus on positive odd integers only and we will prove the statement by strong induction.

Base step: $n = 1$. Clearly, we can write $1 = 2^0 3^0$.

Induction step: Suppose the statement is true for $n = 1, 3, 5, \cdots 2a - 1$ for some integer $a \geq 1$.

Then we want to prove that the statement is true for $n = 1, 3, 5, \cdots 2a - 1, 2(a + 1) - 1 = 2a + 1$.

By induction hypothesis, the statement is true for $n = 1, 3, 5, \cdots 2a - 1$.

It remains to show that the statement is true for $n = 2a + 1$.

Subtract the highest power of 3 that is less than or equal to $2a + 1$, we get $m = 2a + 1 - 3^l$.

Note that $3^l \leq 2a + 1 < 3^{l+1}$ and, hence, $m = 2a + 1 - 3^l < 3^{l+1} - 3^l = 3 \cdot 3^l - 3^l = 2 \cdot 3^l$.

If $m = 0$, then we are done as $2a + 1 = 3^l = 2^0 3^l$.

If $m > 0$, then $2a + 1 - 3^l$ is a positive even integer as $2a + 1$ and 3^l are odd integers.

Hence, by factoring out the highest power of 2 in it, we have $\frac{2a+1-3^l}{2^k} = b$ is a positive odd integer.

Clearly, $b < \frac{2a+1-3}{2} = a - 1 < 2a - 1$.

By induction hypothesis, we can write b as a sum of one or more numbers of the form $2^r 3^s$ where r and s are non-negative integers and no summand divides another.

Hence, we can write $m = 2a + 1 - 3^l$ as a sum of one or more numbers of the form $2^{r+k}3^s$ where r and s are non-negative integers and no summand divides another.

As $m < 2 \cdot 3^l$, all the exponents s in 3^s must be less that l for otherwise $2^{r+k}3^s \geq 2^1 3^l > m$.

Since all the s's are less than l, none of the summand $2^{r+k}3^s$ is divisible by 3^l.

Also, since each of the summand $2^{r+k}3^s$ has a factor of 2 in it, none of them cannot divide 3^l.

Therefore, $2a + 1 = 3^l + \sum 2^{r+k}3^s$ is a sum of the required form with no summand dividing another. This finishes the induction step.

6. (2024 A1) Determine all positive integers n for which there exist positive integers a, b, c such that $2a^n + 3b^n = 4c^n$.

Answer: $n = 1$.

I will let you spot some positive integer solutions for $2a^1 + 3b^1 = 4c^1$.

We will prove that $2a^n + 3b^n = 4c^n$ has no positive integer solution when $n \geq 2$.

When $n = 2$, the equation becomes $2a^2 + 3b^2 = 4c^2$. Suppose a, b, c is a solution with c smallest.

One can check that $x^2 \equiv 0, 1 \pmod 3$. Hence, the above equation leads to $2a^2 \equiv 4c^2 \equiv c^2 \pmod 3$.

For this to be true, we cannot have $a^2 \equiv 1 \pmod 3$ as $2 \cdot 1 \equiv c^2 \pmod 3$ is impossible.

Therefore, we must have $a^2 \equiv 0 \pmod 3$ which implies $a \equiv 0 \pmod 3$.

Then, this implies $2 \cdot 0 \equiv c^2 \pmod 3$. Hence $c \equiv 0 \pmod 3$.

Thus, $a = 3a'$ and $c = 3c'$ for some positive integers a', c'.

Then $2(3a')^2 + 3b^2 = 4(3c')^2$. This implies $18a'^2 + 3b^2 = 36c'^2$ or $b^2 = 12c'^2 - 6a'^2 = 3(4c'^2 - 2a'^2)$.

In particular 3 divides b^2 which implies 3 divides b. Thus, $b = 3b'$ for some positive integer b'.

But then, we have $2(3a')^2 + 3(3b')^2 = 4(3c')^2$.

This gives $2a'^2 + 3b'^2 = 4c'^2$ yielding a solution a', b', c' with a smaller c'.

This contradicts the minimality of c. Hence, there cannot be any positive integer solution to $2a^2 + 3b^2 = 4c^2$.

When $n \geq 3$, we will do a similar but with $\pmod 2$ instead of $\pmod 3$.

Suppose $2a^n + 3b^n = 4c^n$ has some positive integer solution a, b, c with c being smallest.

Then $3b^n = 4c^n - 2a^n$.

Since the right-hand side is even, the left-hand side is also even.

Hence, we must have b is even. Say $b = 2b'$ for some positive integer b'.

Then the equation becomes $2a^n + 3 \cdot 2^n b'^n = 4c^n$ or $a^n = 2c^n - 3 \cdot 2^{n-1} b'^n$.

Since the right-hand side is even, the left-hand side is also even.

Hence, we must have a is even. Say $a = 2a'$ for some positive integer a'.

Then the equation becomes $2 \cdot 2^n a'^n + 3 \cdot 2^n b'^n = 4c^n$ or $2 \cdot 2^{n-2} a'^n + 3 \cdot 2^{n-2} b'^n = c^n$.

Since $n \geq 3$, the left-hand side is even. So, the right-hand side is also even.

Hence, we must have c is even. Say $c = 2c'$ for some positive integer c'.

But then we have $2 \cdot 2^n a'^n + 3 \cdot 2^n b'^n = 4 \cdot 2^n c'^n$ which implies $2a'^n + 3b'^n = 4c'^n$.

This yields positive integer solutions a', b', c' to the same equation but with a smaller c'.

This contradicts the minimality of c. Hence, there cannot be any positive integer solution to $2a^n + 3b^n = 4c^n$ when $n \geq 3$.

7. (2013 A2) Let S be the set of non-perfect squares. For $n \in S$, consider choices of integers $n < a_1 < a_2 < \ldots < a_r$ such that $n \cdot a_1 \cdot a_2 \cdots a_r$ is a perfect square, and let $f(n)$ be the minimum of a_r over all such choices. (e.g., $2 \cdot 3 \cdot 6 = 6^2$ and $f(2) = 6$.) Show that $f : S \to \mathbb{Z}$ is one-to-one.

We will prove by contradiction.

Suppose for two non-perfect squares m and n we have $f(m) = f(n)$. Without loss of generality, say $m < n$.

Say $m \cdot a_1 \cdot a_2 \cdots a_r = f(m)$ is a perfect square with $m < a_1 < a_2 < \ldots < a_r$ and a_r minimum.

Say $n \cdot b_1 \cdot b_2 \cdots b_s = f(n)$ is a perfect square with $n < b_1 < b_2 < \ldots < b_s$ and b_s minimum.

Multiply the above two lists together, we get $m \cdot a_1 \cdot a_2 \cdots a_r \cdot n \cdot b_1 \cdot b_2 \cdots b_s$ which is also a perfect

square as it is the product of two perfect squares.

Now, we can remove any repeated terms among $a_1, a_2, \ldots, a_r, n, b_1, b_2, \ldots, b_s$ (with $a_r = b_s$ being removed at least).

The resulting product $m \cdot \cdots$ is still a perfect square with the largest term less than a_r as a_r and b_s are removed already.

So, we just found a perfect square product $m \cdot \cdots$ with a smaller largest term than that of the perfect square product $m \cdot a_1 \cdot a_2 \cdots a_r$.

This contradicts the minimality of a_r.

Therefore, we cannot have $f(m) = f(n)$ for any two distinct non-perfect squares m, n, and the function f must be one-to-one.