

Putnam practice - Number theory solution

Questions:

1. For any polynomial $p(x)$ with integer coefficients and any two distinct integers a, b , prove that $a - b \mid p(a) - p(b)$.

The key observation is that $a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \cdots + ab^{k-2} + b^{k-1})$.

Let $p(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 = \sum_{i=0}^n c_i x^i$.

Then $p(a) - p(b) = \sum_{i=0}^n c_i (a^i - b^i) = \sum_{i=0}^n (a - b)(a^{i-1} + a^{i-2}b + \cdots + ab^{i-2} + b^{i-1}) = (a - b) \sum_{i=0}^n (a^{i-1} + a^{i-2}b + \cdots + ab^{i-2} + b^{i-1})$ which has a factor $a - b$.

2. Let $p(x)$ be a polynomial with integer coefficients and degree at least 1. Prove that $p(n)$ is a composite number for infinitely many integers n .

Suppose $p(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0$ and we may assume $c_n > 0$ without loss of generality (for otherwise one can consider $-p(x)$ instead).

Since $p(x)$ has degree at least 1 and positive leading coefficient, $p(x) \rightarrow \infty$ and $p'(x) > 0$ as $x \rightarrow \infty$.

Thus, for some big integer N , $p(N) > 1$ and $p(x)$ is increasing for $x \geq N$.

By question 1, $p(N) = p(N) + N - N \mid p(p(N) + N) - p(N)$. Hence, $p(N) \mid p(p(N) + N)$.

Repeat the process, $p(p(N) + N) = p(p(N) + N) + (p(N) + N) - (p(N) + N) \mid p(p(p(N) + N) + (p(N) + N)) - p(p(N) + N)$. Thus, $p(N) \mid p(p(N) + N) \mid p(p(p(N) + N) + (p(N) + N))$.

One can repeat the process and create infinitely many $P(*)$ that are divisible by $p(N)$, and, hence, are composite.

3. (2017) Let f be a polynomial with positive integer coefficients. Prove that if n is a positive integer, then $f(n)$ divides $f(f(n) + 1)$ if and only if $n = 1$.

Suppose $f(x) = c_m x^m + c_{m-1} x^{m-1} + \cdots + c_1 x + c_0$.

Then $f(n) = c_m n^m + c_{m-1} n^{m-1} + \cdots + c_1 n + c_0$ and

$$\begin{aligned} f(f(n) + 1) &= c_m (f(n) + 1)^m + c_{m-1} (f(n) + 1)^{m-1} + \cdots + c_1 (f(n) + 1) + c_0 \\ &\equiv c_m 1^m + c_{m-1} 1^{m-1} + \cdots + c_1 1 + c_0 = f(1) \pmod{f(n)}. \end{aligned}$$

Clearly, when $n = 1$, the above gives $f(f(1) + 1) \equiv f(1) \equiv 0 \pmod{f(1)}$. So, $f(n)$ divides $f(f(n) + 1)$ if $n = 1$.

When $n > 1$, since the coefficients are positive integers, we have $0 < f(1) < f(n)$. So, when $f(f(n) + 1)$ is divided by $f(n)$, it has a non-zero remainder $f(1)$. Therefore, $f(f(n) + 1)$ is not divisible by $f(n)$ in all these other cases $n > 1$.

This proves that $f(n)$ divides $f(f(n) + 1)$ if and only if $n = 1$.

4. (1969) Let n be a positive integer such that 24 divides $n + 1$. Prove that the sum of all the positive divisors of n is divisible by 24.

One can rewrite $24 \mid n + 1$ as $n \equiv -1 \pmod{24}$. Or equivalently $n \equiv -1 \pmod{3}$ and $n \equiv -1 \pmod{8}$ by Chinese remainder theorem.

In particular, $n \not\equiv 0, 1 \pmod{4}$. Hence, n is not a perfect square.

Now, one can pair up the divisors of n as follows: For any $d \mid n$ with $1 \leq d < \sqrt{n}$, we can pair it up with $\sqrt{n} < \frac{n}{d} \leq n$. (Note: Since n is not a perfect square, it does not have a divisor $d = \sqrt{n}$.)

If $d \equiv 1 \pmod{3}$, then $\frac{n}{d} \equiv -1 \pmod{3}$ since $d \cdot \frac{n}{d} = n \equiv -1 \pmod{3}$.

If $d \equiv -1 \pmod{3}$, then $\frac{n}{d} \equiv 1 \pmod{3}$ since $d \cdot \frac{n}{d} = n \equiv -1 \pmod{3}$.

In any case, $d + \frac{n}{d} \equiv 1 - 1 \equiv 0 \pmod{3}$.

Since 2 divides $n + 1$, n is odd and $n \equiv 1, 3, 5, 7 \equiv 1, 3, -3, -1 \pmod{8}$.

If $d \equiv 1 \pmod{8}$, then $\frac{n}{d} \equiv -1 \pmod{8}$ since $d \cdot \frac{n}{d} = n \equiv -1 \pmod{8}$.

If $d \equiv 3 \pmod{8}$, then $\frac{n}{d} \equiv -3 \pmod{8}$ since $d \cdot \frac{n}{d} = n \equiv -1 \pmod{8}$.

If $d \equiv -3 \pmod{8}$, then $\frac{n}{d} \equiv 3 \pmod{8}$ since $d \cdot \frac{n}{d} = n \equiv -1 \pmod{8}$.

If $d \equiv -1 \pmod{4}$, then $\frac{n}{d} \equiv 1 \pmod{4}$ since $d \cdot \frac{n}{d} = n \equiv -1 \pmod{4}$.

In any case, $d + \frac{n}{d} \equiv 1 - 1 \equiv 0 \pmod{4}$.

Combining the two congruences $\pmod{3}$ and $\pmod{4}$, we get $d + \frac{n}{d} \equiv 0 \pmod{24}$.

Summing over $1 \leq d < \sqrt{n}$, we get the sum of all positive divisors of n is $\equiv 0 \pmod{24}$ (i.e., divisible by 24).

5. (2010) Prove that for each positive integer n , the number $10^{10^{10^n}} + 10^{10^n} + 10^n - 1$ is not prime.

First, consider $n = 1$. Note that $10 \equiv -1 \pmod{11}$.

Then $10^{10^{10^1}} + 10^{10^1} + 10^1 - 1 \equiv (-1)^{10^{10^1}} + (-1)^{10^1} + (-1)^1 - 1 \equiv 0 \pmod{11}$ since the first two exponents of -1 are even.

It is not prime as it has a divisor 11 and the number itself is clearly greater than 11.

When $n = 2$. Note that $10^2 \equiv -1 \pmod{101}$.

Then $10^{10^{10^2}} + 10^{10^2} + 10^2 - 1 = 10^{2 \cdot 5 \cdot 10^{10^2-1}} + 10^{2 \cdot 5 \cdot 10} + 10^2 - 1 = (10^2)^{5 \cdot 10^{10^2-1}} + (10^2)^{5 \cdot 10} + 10^2 - 1 \equiv 1 + 1 - 1 - 1 \equiv 0 \pmod{101}$.

In general, suppose $n = 2^a \cdot b$ where 2^a is the highest power of 2 that divides n . Hence, b is odd.

We try to consider things modulo $10^{2^a} + 1$. Then

$$\begin{aligned}
10^{10^{10^n}} + 10^{10^n} + 10^n - 1 &= 10^{10^{10^{2^a \cdot b}}} + 10^{10^{2^a \cdot b}} + 10^{2^a \cdot b} - 1 \\
&= 10^{2^a \cdot 2^{10^{2^a \cdot b} - a} \cdot 5^{10^{2^a \cdot b}}} + 10^{2^a \cdot 2^{2^a \cdot b - a} \cdot 5^{2^a \cdot b}} + (10^{2^a})^b - 1 \\
&= (10^{2^a})^{2^{10^{2^a \cdot b} - a} \cdot 5^{10^{2^a \cdot b}}} + (10^{2^a})^{(2^{2^a \cdot b - a} \cdot 5^{2^a \cdot b})} + (10^{2^a})^b - 1 \\
&\equiv 1 + 1 + (-1) - 1 \equiv \pmod{10^{2^a} + 1}
\end{aligned}$$

as the first two exponents of (10^{2^a}) are even by noting that $10^{2^a \cdot b - a} \geq 10^{2^a - a} \geq 1$ and $2^{2^a \cdot b} - a \geq 2^{2^a} - a \geq 1$.

6. (1972) For all integer $n > 1$, prove that n does not divide $2^n - 1$.

First, observe that $2^n - 1$ is an odd integer. Hence, it is not divisible by 2 and, hence, not divisible by n if n is even.

From now on, we can restrict our attention to odd integer $n > 1$.

Suppose the contrary that n divides $2^n - 1$.

Let p be the smallest prime factor of n . Then $2^n \equiv 1 \pmod{p}$.

Then $n = p^a \cdot m$ for some positive integer a and positive integer m with $p \nmid m$.

Note that $2^p \equiv 2 \pmod{p}$ by Fermat's little theorem. This implies $2^{p^2} = (2^p)^p \equiv (2)^p \equiv 2 \pmod{p}$. By induction, one can prove that $2^{p^k} \equiv 2 \pmod{p}$ (I will let you try it).

Consequently, $1 \equiv 2^n = (2^{p^a})^m \equiv (2)^m \pmod{p}$.

By Fermat little theorem, we have $2^{p-1} \equiv 1 \pmod{p}$ and let k be the smallest positive integer such that $2^k \equiv 1 \pmod{p}$.

Clearly $k > 1$ as $2 \not\equiv 1 \pmod{p}$ for $p \geq 3$.

Also, we must have $k \mid m$ for otherwise $m = kq + r$ for some $1 \leq r < k$. We would have $1 \equiv 2^m \equiv 2^{kq+r} \equiv (2^k)^q \cdot 2^r \equiv 1 \cdot 2^r \pmod{p}$, yielding a smaller integer r than k with $2^r \equiv 1 \pmod{p}$.

Similarly, we must have $k \mid p - 1$ for otherwise $p - 1 = kq' + r'$ for some $1 \leq r' < k$. We would have $1 \equiv 2^{p-1} \equiv 2^{kq'+r'} \equiv (2^k)^{q'} \cdot 2^{r'} \equiv 1 \cdot 2^{r'} \pmod{p}$, yielding a smaller integer r' than k with $2^{r'} \equiv 1 \pmod{p}$.

So, $k > 1$ has prime factors smaller than or equal to $p - 1$.

This implies that m has a prime factor smaller than p which contradicts p being the smallest prime factor of $n = p^a \cdot m$.

Therefore, n does not divide $2^n - 1$.

7. (1994) For any integer a , set $n_a = 101a - 100 \cdot 2^a$. Show that for $0 \leq a, b, c, d \leq 99$, $n_a + n_b \equiv n_c + n_d \pmod{10100}$ implies $\{a, b\} = \{c, d\}$.

Lemma: If n is the smallest positive integer such that $2^n \equiv 1 \pmod{101}$, then $n = 100$. In particular, for all integers $0 \leq x < y \leq 99$, we have $2^x \not\equiv 2^y \pmod{101}$.

Proof: By Fermat's little theorem, $2^{100} \equiv 1 \pmod{101}$.

Now, suppose $100 = n \cdot q + r$ for some quotient q and remainder $0 \leq r < n$.

Then, we have $1 \equiv 2^{100} \equiv 2^{n \cdot q + r} \equiv (2^n)^q \cdot 2^r \equiv 1 \cdot 2^r \pmod{101}$ as $2^n \equiv 1 \pmod{101}$.

However, $r < n$. This would contradict n being the smallest positive integer such that $2^n \equiv 1 \pmod{101}$ unless $r = 0$.

Therefore, n must divide 100 (i.e., $n = 1, 2, 4, 5, 10, 20, 25, 50, 100$).

One can check that $2^1 \equiv 2 \pmod{101}$, $2^2 \equiv 4 \pmod{101}$, $2^4 \cdot 4^2 \equiv 16 \pmod{101}$, $2^5 \equiv 32 \pmod{101}$, $2^{10} \equiv 1024 \equiv 14 \pmod{101}$, $2^{20} = (2^{10})^2 \equiv 14^2 \equiv 95 \pmod{101}$, $2^{25} = 2^{20} \cdot 2^5 \equiv 95 \cdot 32 \equiv 10 \pmod{101}$, $2^{50} = (2^{25})^2 \equiv 10^2 \equiv 100 \pmod{101}$.

None of the above is $\equiv 1 \pmod{101}$. Therefore, $n = 100$ is the smallest positive integer such that $2^n \equiv 1 \pmod{101}$.

For the last part of the lemma, suppose the contrary that $2^x \equiv 2^y \pmod{101}$ for some $0 \leq x < y \leq 99$.

Then $0 \equiv 2^y - 2^x = 2^x(2^{y-x} - 1) \pmod{101}$.

Since $\gcd(2, 101) = 1$, this implies $2^{y-x} \equiv 1 \pmod{101}$ which is a contradiction as $0 < y - x \leq 99 - 0 < 100$.

Proof of question 7: By definition of n_a , the equation $n_a + n_b \equiv n_c + n_d \pmod{10100}$ becomes

$$101a - 100 \cdot 2^a + 101b - 100 \cdot 2^b \equiv 101c - 100 \cdot 2^c + 101d - 100 \cdot 2^d \pmod{10100}.$$

Since $10100 = 101 \cdot 100$ with $\gcd(101, 100) = 1$, it is equivalent to consider the above equation modulo 100 and 101 by the Chinese Remainder Theorem.

Hence, we obtain

$$101a + 101b \equiv 101c + 101d \pmod{100} \text{ and } -100 \cdot 2^a - 100 \cdot 2^b \equiv -100 \cdot 2^c - 100 \cdot 2^d \pmod{101}$$

which reduce to

$$a + b \equiv c + d \pmod{100} \text{ and } 2^a + 2^b \equiv 2^c + 2^d \pmod{101}$$

since $101 \equiv 1 \pmod{100}$ and $-100 \equiv 1 \pmod{101}$.

Thus, $(c + d) = (a + b) + 100k$ for some integer k .

By Fermat's little theorem, we know that $2^{100} \equiv 1 \pmod{101}$ as 101 is prime and $\gcd(2, 101) = 1$.

Thus, $2^{c+d} \equiv 2^{(a+b)+100k} \equiv 2^{a+b} \equiv 2^e \pmod{101}$ for some $1 \leq e \leq 100$ by Lemma (i.e., $e \equiv a + b \equiv c + d \pmod{100}$.)

For positive integer n , we denote $2^{-n} \pmod{101}$ as the congruence class $x_n \pmod{101}$ such that $2^n \cdot x_n \equiv 1 \pmod{101}$.

Then $2^a + 2^e \cdot 2^{-a} \equiv 2^c + 2^e \cdot 2^{-c} \pmod{101}$. This implies $2^a - 2^c \equiv 2^e \cdot 2^{-c} - 2^e \cdot 2^{-a} \equiv 2^{e-c-a} \cdot (2^a - 2^c) \pmod{101}$.

If $a = c$, then it follows from $a + b \equiv c + d \pmod{100}$ that $b \equiv d \pmod{100}$ and $b = d$ as $0 \leq b, d \leq 99$. We have $\{a, b\} = \{c, d\}$ in this case.

If $a \neq c$. By Lemma, $2^a \not\equiv 2^c \pmod{101}$ or $2^a - 2^c \not\equiv 0 \pmod{101}$.

So, the congruence $2^a - 2^c \equiv 2^{e-c-a}(2^a - 2^c) \pmod{101}$ can be simplified to $1 \equiv 2^{e-c-a} \pmod{101}$ by Euclid's lemma.

By Lemma again, we must have $e - c - a \equiv 0 \pmod{100}$ or $e - c \equiv a \pmod{100}$. This implies $d = (c + d) - c \equiv a \pmod{100}$.

Since $0 \leq a, d \leq 99$, we must have $d = a$.

It follows from $a + b \equiv c + d \pmod{100}$ that $b \equiv c \pmod{100}$ and $b = c$ as $0 \leq b, c \leq 99$. We also have $\{a, b\} = \{c, d\}$ in this case.