Targil 1 - polynomials.

1. A polynomial $p(x)$ of degree n has only integer values in integer points.
(a) Show that $n!p(x)$ has integer coefficients.
(b) Can we claim that $p(x)$ has integer coefficients?

Solution.
(b) No. For example $p(x) = x(x+1)/2$ or, more generally, the binomial coefficient $p(x) = x(x-1)(x-2)\ldots(x-n+1)/n!$ (By the way, why is it integer for integer x?)

(a) For every k from 0 to n consider a polynomial

$$p_k(x) = \frac{x}{k}\cdot\frac{x-1}{k-1}\cdot\frac{x-2}{k-2}\cdot\ldots\cdot\frac{x-k+1}{1}\cdot\frac{x-k-1}{-1}\cdot\ldots\cdot\frac{x-n}{k-n}.$$

This polynomial is equal 1 at k and 0 at all other integer points from 0 to n.
And all these polynomial have degree n.
For each polynomial $p(x)$ of degree n consider polynomial

$$q(x) = p(0)\,p_0(x) + p(1)\,p_1(x) + p(2)\,p_2(x) + \ldots + p(n)\,p_n(x)$$

Notice, that $p(x), q(x)$ coincide at 0, 1, 2, … , n so $p(x) - q(x)$ have at least $n+1$ roots, that it impossible for polynomial of degree n unless it is identically zero.
So $q(x)$ is $p(x)$.
Hence it is enough to show that $n!q(x)$ or even $n!\,p_k(x)$, has integer coefficients.

$$n!\,p_k(x) = \pm\frac{n!}{k!(n-k)!}x(x-1)(x-2)\ldots(x-k+1)(x-k-1)\cdot\ldots\cdot(x-n)$$

And $\dfrac{n!}{k!(n-k)!}$ is integer (did I ask You how to prove that)?

2. Let $p(x)$ be a polynomial with integer coefficients, and $a_1 < a_2 < \ldots < a_n$ integer numbers.
(a) Prove that there always exists an integer a such that $p(a)$ is divisible by $p(a_1)$, $p(a_2)$, … , $p(a_n)$.
(b) Can we claim that there always exists an integer a such that $p(a)$ is divisible by $p(a_1)p(a_2)\cdot\ldots\cdot p(a_n)$?

Solution. (b) No. $p(n) = 4n + 2$ is always divisible by 2 and never divisible by 4.
(a) It is enough to prove for $n = 2$ (that there is a such that $p(a)$ is divisible by $p(a_1)$ and $p(a_2)$), and then the statement is obvious by induction.

The most useful lemma about polynomials with integer coefficients:
$p(x) - p(y)$ is divisible by $x - y$.

Since that fact is so important, we shal see 2 proofs:
First proof. $x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \dots xy^{n-1})$ is divisible by $x - y$.
So sums of those expressions with integer coefficientsare also divisible by $x - y$.
Second proof. $x = y \pmod{x - y}$ hence $x^n = y^n \pmod{x - y}$ for all n,
therefore $p(x) = p(y) \pmod{x - y}$

So, back to the problem. All $p(a_1 + kp(a_1))$ are divisible by $p(a_1)$, while all $p(a_2 + mp(a_2))$ are divisible by $p(a_2)$. So if $a_1 + kp(a_1) = a = a_2 + mp(a_2)$, we won. By the inverse part of Euclidean algorithm, we know we can do it if $p(a_1)$, $p(a_2)$ are coprime (don't have a common divisor > 1).

If they are not coprime, "make them coprime". Let s be a product of all highest powers of primes in the decomposition of $p(a_1)$ which are higher than corresponding powers in the decomposition of $p(a_2)$. Let t be the product of all highest powers of all other primes in the decomposition of $p(a_1)$.
Then $\gcd(s, t) = 1$, while $\text{lcm}(s, t) = \text{lcm}(p(a_1), p(a_2))$
(Here lcm is the least common multiple, gcd is the greatest common divisor.)
Then we can find a such that $a_1 + ks = a = a_2 + mt$, then $p(a)$ is divisible by st which is lcm(s, t) which is the same as $\text{lcm}(p(a_1), p(a_2))$. That's it.

3. Let $P(x)$ be polynomial with integer coefficients of degree $n > 1$.
Consider a polynomial $Q(x) = P(P(P(\dots P(P(x))\dots)))$, where P occurs n times.
Show that Q has no more than n integer stable points, i. e. no more than n integers such that $Q(z) = z$.

Solution. It follows from the most useful lemma on polynomials with integer coefficients (at the top of this page) that applying P to two different integers performs one of the following 3 operations:

a. Glues them together
b. Keeps the distance between them
c. Magnifies the distance between them.

Consider two stable points of $P(P(P(\dots)))$. Each time we apply P to both points, they cannot be glued together, and cannot become more distant (since afterwards after applying P more times they won't get closer unless they'll be glued together). So P keeps the distance between each two stable points of $P(P(P(\dots)))$.

So, if we have several stable points of $P(P(P(\ldots)))$, then P keeps distance between them all, so action of P on that set of points is the same as action of a linear function $L(x)$ of slope 1 or -1. So all those points satisfy the equation $P(x) = L(x)$. But this is polynomial equation of degree n, so it has no more than n roots.

4. Consider a graph of a polynomial $p(x)$ of degree n on a plane, and a point P on the same plane. Show that there are no more than n tangent lines to the graph of $p(x)$ passing through P.

Solution. Shifting in both x and y direction doesn't influence the degree of polynomial, so we may assume that P is the origin (0, 0).
The equation of tangent line to $p(x)$ at $(z,p(z))$ is $y - p(z) = (x - z)\, p'(z)$
If it passes via 0 we get $-p(z) = -z\, p'(z)$
That is a polynomial equation of z of degree n.
It cannot have more than n solution!
Unless… it is constantly 0.
But the highest degree term coefficient in the left hand side is $-az^n$ and in the right hand side is $-naz^n$ and they don't cancel out, unless $n = 1$ and then degree is 1 and tangent line is unique (though there are infinite number of tangent points).

5*. Prove that $5765^{5765}+5766$
(a) is not a prime number
(b) is a product of three numbers which are greater than 1.

Solution. (a) $5765 = 5600 + 140 + 21 + 4 = 4 \pmod 7$.

$4^3 = 2^6 = 1 \pmod 7$ because of Fermat little theorem.

$5765 = 2 \pmod 3$ so

$5765^{5765}+5766 = 4^2 + 5 = 0 \pmod 7$

So, it is divisible by 7.

(b) Polynomial $x^{3n+2} + x + 1$ accepts zero values at $\frac{1 \pm \sqrt{3}}{2}$ (those are the numbers such that $x^3 = 1$ but $x \neq 1$, i. e. $\frac{x^3 - 1}{x - 1} = x^2 + x + 1$).

Since the set of roots of $x^{3n+2} + x + 1$ contains the set of roots of $x^2 + x + 1$ and the last has roots of multiplicity 1, the first is divisible by the last. Since the first coefficient of the last is 1 and other coefficients of both polynomials are integer, we see that the result of division will be a polynomial with integer coefficients.

Therefore $5765^{5765}+5766$ is divisible by $5765^2 + 5766$. QED.