Math 299 **Recitation 9** **Oct 31, 2013**

1. PROPOSITION: For every positive integer n, the polynomial $x - y$ divides $x^n - y^n$.

a. Assume this proposition is true, use it to prove the following: 7 divides $12^n - 5^n$, 4 divides $5 \cdot 7^n - 3^n$, and 4 divides $3 \cdot 7^n + 5 \cdot 3^n$.

First is a direct application of the proposition with $x = 12$ and $y = 5$. All we need to verify is that $x - y = 7$.

For the second: $5 \cdot 7^n - 3^n = 4 \cdot 7^n + (7^n - 3^n)$. First term is a multiple of 4, and by the proposition the second term is also a multiple of 4, hence the sum is a multiple of 4.

For the third: $3 \cdot 7^n + 5 \cdot 3^n = 3 \cdot 7^n + 5 \cdot 3^n - 3 \cdot 3^n + 3 \cdot 3^n = 3(7^n - 3^n) + 8 \cdot 3^n$ where first term is divisible by 4 using the proposition and the second term is a multiple of 8, hence a multiple of 4, so the sum is a multiple of 4.

b. (Optional) Prove the proposition using induction on n. (Hint: Try to create a term with a factor $(x^n - y^n)$)

Check for $n = 0$, $x - y$ divides $1 - 1 = 0$, which holds.

Assume true for $n = k$: $x - y | x^k - y^k$, which means $x^k - y^k = (x - y) \cdot P(x, y)$ for some polynomial P in variables x and y and with integer coefficients.

For $n = k + 1$: $x^{k+1} - y^{k+1} = x \cdot x^k - y \cdot y^k$, we want to find a term with a factor $(x^n - y^n)$

$$= x \cdot x^k - \mathbf{x} \cdot \mathbf{y^k} + \mathbf{x} \cdot \mathbf{y^k} - y \cdot y^k$$
$$= x \cdot (x^k - \mathbf{y^k}) + \mathbf{x} \cdot \mathbf{y^k} - y \cdot y^k$$
$$= x \cdot (x^k - \mathbf{y^k}) + y^k(\mathbf{x} - y) = (x - y)(P(x, y) - y).$$

2. Prove that if $gcd(a, b) = 1$ and $c|b$ then $gcd(a, c) = 1$. (Hint: Use proof by contradiction)

Assume the contrary: $gcd(a, b) = 1$ and $c|b$ **and** $gcd(a, c) > 1$

Since $gcd(a, b) = 1$, b is nonzero, since $c|b$, we also have c is nonzero.

Let $gcd(a, c) = d > 1$. Then $a = d \cdot k$ and $c = d \cdot l$.

Since $c|b$, we can write $b = c \cdot m = (d \cdot l) \cdot m$ for some integer m.

We see that d is a common divisor of a and b greater than 1, which contradicts with the original assumption that $gcd(a, b) = 1$.

3. Given two positive integers a, b consider the set $B = \{m \cdot a + n \cdot b \mid m, n \in \mathbb{Z}, m \cdot a + n \cdot b > 0\}$, and let d be the smallest element in B (Why does it exist?).

Prove that d divides a. (Hint: use proof by contradiction and the division lemma)

Let $d = u \cdot a + v \cdot b$.

Assume that d doesn't divide a, then there is a remainder: $a = q \cdot d + r$ with $0 \leq r < d$.

Solving for r, we get $r = a - q \cdot d = a - q(u \cdot a + v \cdot b) = (1 - qu)a + (-qv)b$ which is an element of B, but $r < d$ which contradicts with the fact that d was the smallest element.

Remark: B is nonempty because for $m = 1, n = 0$ we see that $a \in B$ since a itself is a positive integer.

4. (a) Let $A = \{k^2 \mid k \in \mathbb{N}, k > 2\}$. Show that $x \in A \Rightarrow x|(x - 1)!$. $(4! = 4 \cdot 3 \cdot 2 \cdot 1)$

Check that $k < k^2 - 1$ and $2k < k^2 - 1$ if $k > 2$. Therefore k and $2k$ are distinct factors in $(k^2 - 1)!$. After rearranging we see $(k^2 - 1)! = k \cdot (2k) \cdot m$ where m is the product of all integers between 1 and $k^2 - 1$ except k and $2k$.

(b) (Optional) Find the largest subet of $\mathbb{N}$ for which the same statement is true.

Claim: All composite numbers greater than 4.

Need to show: (1) true for composite numbers x that are not squares, and (2) false for prime numbers x.

(1) Write $x = a \cdot b$ with $1 < a < b$ or $1 < b < a$ and both are less than x,
hence without loss of generality we can assume $x = a \cdot b$ with $1 < a < b < x - 1$. (First and last inequalities are strict because $a \neq 1$ since x is composite. Again a and b are distinct factors in $(x - 1)!$.

(2) Follows from the definition of prime numbers and Euclid's lemma: if p divides the product $(x - 1)(x - 2) \cdots 2 \cdot 1$ then it has to divide one of the factors, but all factors are less than p.

5. EUCLID'S LEMMA: Suppose that $n, a, b \in \mathbb{N}$. If $n|a \cdot b$ and $gcd(n, a) = 1$ then $n|b$.
Use Euclid's Lemma to prove that if a prime p divides $a \cdot b$ then p divides a or p divides b.
Case 1: $gcd(p, a) = 1$. If p divides $a \cdot b$, then by Euclid's lemma p divides b.
Case 2: $gcd(p, a) > 1$. In this case $gcd(p, a) = p$ since the only number that divides p greater than 1 is p itself. Hence p divides a.

6. (a) Use the Euclidean algorithm to compute $gcd(2013, 405)$. Show your steps.
$2013 = 4 \cdot 405 + 393$ $\quad$ $5 \cdot 405 = 2025$ which is too much, use $4 \cdot 405 = 1620$
$405 = 1 \cdot 393 + 12$
$393 =? \cdot 12+?$ $\quad$ $30 \cdot 12 = 360, 31 \cdot 12 = 372, 32 \cdot 12 = 384$
so
$393 = 32 \cdot 12 + 9$ $\quad$ hence (**) $9 = 393 - 32 \cdot 12$
$12 = 1 \cdot 9 + 3$ $\quad$ hence (*) $3 = 12 - 1 \cdot 9$
$9 = 3 \cdot 3 + 0$ hence gcd is the previous remainder.
(b) Use the solution to part (a) to find an integer solution (X, Y) for the equation $2013x + 405y = 15$. Is the solution unique?
$15 = 5 \cdot gcd(2013, 405)$, hence start to write 15 in terms of the remainders in the above computation:
$15 = 5 \cdot 3$
$= 5 \cdot (12 - 1 \cdot 9)$ by (*)
$= 5(12 - 1 \cdot (393 - 32 \cdot 12)) = 5(33 \cdot 12 - 393)$ by (**) and combining like terms
$= 5(33(405 - 1 \cdot 393) - 393) = 5(33 \cdot 405 - 34 \cdot 393)$
$= 5(33 \cdot 405 - 34(2013 - 4 \cdot 405)) = 5((33 + 34 \cdot 4)405 - 34 \cdot 2013)$
$= 2013(-5 \cdot 34) + 405(5 \cdot (33 + 34 \cdot 4))$

The solution is not unique, we can increase x by $405/3$ and decrease y by $2013/3$ and get a new solution. All other solutions are obtained similarly.