MATH 240: Discrete structures I. Fall 2011

Assignment #3: Number theory. Solutions.

1. *Prime factorization.* Show that $\sqrt[3]{3}$ is irrational.

Solution: Suppose for a contradiction that $\sqrt[3]{3} = \frac{m}{n}$ for some positive integers m and n. Then $3n^3 = m^3$. Let k be the power of 3 in the (unique) prime factorization of n, and let l be such power in the prime fatorization of m. Then the power of 3 in the prime factorization of $3n^3$ is $3k+1$, and it is $3l$ in the factorization of m^3. We get $3k+1 = 3l$, which is a contradiction as the right side is divisible by 3 and the left side is not.

2. *Euclid's algorithm.* Use the Euclid's Algorithm to find each of the following.

(a) $\gcd(1230, 96)$;

(b) $\gcd(34, 411)$.

Solution (a):

$$\begin{aligned} 1230 &= 96 \cdot 12 + 78 \\ 96 &= 78 \cdot 1 + 18 \\ 78 &= 18 \cdot 4 + 6 \\ 18 &= 6 \cdot 3 \end{aligned}$$

$\gcd(1230, 96) = 3$.

b):

$$\begin{aligned} 411 &= 34 \cdot 12 + 3 \\ 34 &= 3 \cdot 11 + 1 \end{aligned}$$

$\gcd(34, 411) = 1$.

3. *Congruences.* Evaluate the following.

(a) $36^{1620} (\bmod 17)$

(b) $36^{1620} (\bmod 30)$

Solution (a): By Fermat's little theorem $36^{16} \equiv 1 \pmod{17}$. $1620 = 16 * 101 + 4$. Therefore,

$$36^{1620} \equiv 36^4 \equiv 2^4 = 16 \pmod{17}.$$

(b): $36 \equiv 6 \pmod{30}$ and $6 \cdot 6 \equiv 6 \pmod{30}$. It follows that $36^k \equiv 6 \pmod{30}$ for every positive integer k, and, in pariticular, for $k = 1620$.

4. *Modular equations.* Solve the following equations.

(a) $5x + 1 \equiv 0 \pmod{13}$;

(b) $17x - 5 \equiv 0 \pmod{211}$;

(c) $x^2 - 3x + 2 \equiv 0 \pmod{17}$.

Solution: (a) $5 \cdot 8 - 13 \cdot 3 = 1$. Therefore $5 \cdot 8 \equiv 1 \pmod{13}$.

$$\begin{aligned} 5x &\equiv -1 \pmod{13} \\ 8 \cdot 5x &\equiv 8 \cdot (-1) \pmod{13} \\ x &\equiv -8 \equiv 5 \pmod{13}. \end{aligned}$$

b): Using Eucledian algorithm we obtain $5 \cdot 211 - 62 \cdot 17 = 1$, and $(-62) \cdot 17 \equiv 1 \pmod{211}$. As in (a), we get $x \equiv (-62) \cdot 5 = -310 \equiv 112 \pmod{211}$.

c):

$$\begin{aligned} x^2 - 3x + 2 &\equiv 0 \pmod{17} \\ (x-1)(x-2) &\equiv 0 \pmod{17} \\ x &\equiv 1, 2 \pmod{17}. \end{aligned}$$

5. *Proofs.*

(a) Show that for all integers a, b and k we have

$$\gcd(a, b) = \gcd(b, a - kb).$$

(b) Show that for all positive integers m and n

$$\gcd(2^m - 1, 2^n - 1) = 2^{\gcd(m,n)} - 1.$$

Solution: a) Let $d_1 = \gcd(a, b)$ and let $d_2 = \gcd(b, a - kb)$. We have $d_1|a$ and $d_1|b$, therefore $d_1|a - kb$ and consequently $d_1|d_2$. On the other hand, $d_2|b$ and $d_2|a - kb$, therefore $d_2|(a - kb) + k \cdot b = a$. It follows that $d_2|d_1$. Thus, $d_1 = d_2$, as required.

b): Suppose not. Let m, n be the pair of positive integers for which the formula does not hold chosen with $m + n$ as small as possible and with $m > n$. (If $m = n$ the formula is clearly correrct.) Using part (a) we have,

$$\gcd(2^m - 1, 2^n - 1) = \gcd(2^n - 1, 2^m - 1 - 2^{m-n}(2^n - 1)) = \gcd(2^n - 1, 2^{m-n} - 1).$$

As $n + (m - n) = m < m + n$, by the choice of m and n as the counterexample with the smallest sum, we have

$$\gcd(2^n - 1, 2^{m-n} - 1) = 2^{\gcd(n, m-n)} - 1 = 2^{\gcd(m,n)} - 1,$$

where we used the result of part (a) again in the last equality. Therefore the formula is correct fro m and n, contradicting existence of a counterexample.