Discrete Mathematics, 2016 Fall - Worksheet 18

November 30, 2016

Instructor: Zsolt Pajor-Gyulai, CIMS

In all of the above problems explain your answer in full English sentences.

1. Solve the single congruence
$$7k \equiv 3 \text{ (mod 11)}$$
Note that $7^{-1} = 8$ in $\mathbb{Z}_1 1$. Therefore $k_0 = 7^{-1} \otimes 3 = 8 \otimes 3 = 2$ and the general solution of the congruence is given by
$$k = 2 + 11j, \qquad j \in \mathbb{Z}$$

2. Solve the following system of equation
$$x \equiv 4 \text{ (mod 5)}, \qquad x \equiv 7 \text{ (mod 11)}$$
By the first congruence, we get $x = 4 + 5k$ for some integer k. Plugging this back into the second one we get
$$4 + 5k \equiv 7 \ (11) \qquad \to \qquad 5k \equiv 3 \ (11)$$
Since $5^{-1} = 9$, we have that $k_0 = 9 \otimes 3 = 5$ and therefore
$$k = 5 + 11j \qquad j \in \mathbb{Z},$$
which implies
$$x = 4 + 5(5 + 11j) = 29 + 55j \qquad j \in \mathbb{Z}$$

3. Factor the following positive integers into primes.
   (a) $25 = 5 \cdot 5$
   (b) $4200 = 2 \cdot 2100 = 2 \cdot 3 \cdot 7 \cdot 100 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$
   (c) $10^{10} = 2^{10} \cdot 5^{10}$
   (d) $19 = 19$
   (e) $1 = 1$

4. Let a and b be positive integers. Prove that a and b are relatively prime if and only if there is no prime p such that $p|a$ and $p|b$.

Proof. The only if part is easy, we prove the contrapositive, i.e. that the existence of a prime p with $p|a$ and $p|b$ implies that a and b are not relatively prime. But this is straightforward because then p is a common divisor of a and b and therefore $gcd(a, b) \geq p$.

To prove the if part assume that there are no primes dividing both a and b. If the prime factorizations are

$$a = \ldots p^{\alpha} \ldots, \qquad b = \ldots p^{\beta} \ldots.$$

then clearly either α or β are zero and hence $\min(\alpha, \beta) = 0$ for all primes p. By the formula for the gcd in terms of prime factorizations, this clearly implies $gcd(a, b) = 1$. □

5. Let a and b be positive integers. Prove that 2^a and $2^b - 1$ are relatively prime by considering their prime factorizations.

   Proof. Note that the prime factorization of 2^a consists only of 2-s. However $2^b - 1$ is an odd number and therefore there are no 2-s in their prime factorization. □

6. Prove that if $a, p \in \mathbb{Z}$ with p prime and $p|a^2$, then $p|a$.

   Proof. Note that $p|a^2$ is $p|a \cdot a$ and by the auxiliary lemma in class, we get $p|a$. □