Homework #2. Solutions to selected problems.

1. Let $n_1, \ldots, n_k$ and m be positive integers, and let $n = n_1 n_2 \ldots n_k$.

(a) Assume that $gcd(n_i, m) = 1$ for each $1 \leq i \leq k$. Prove that $gcd(n, m) = 1$.

(b) Now assume that $n_i \mid m$ for each $1 \leq i \leq k$ and $gcd(n_i, n_j) = 1$ for $i \neq j$. Prove that $n \mid m$.

Note that both (a) and (b) were used in the proof of the Chinese Remainder Theorem (CRT). Also note that part (b) in the case $k = 2$ is simply the assertion of Corollary 1.11(a) from the book.

Solution: (a) We will use the fact (established in Lecture 2) that a congruence $ax \equiv b \mod k$ has a solution $\iff gcd(a, k) \mid b$.

We are given that $gcd(n_i, m) = 1$ for each i. Thus, by the above fact there exist $x_i \in \mathbb{Z}$ such that $n_i x_i \equiv 1 \mod m$. Multiplying these congruences over all i, we get $n(\prod_{i=1}^{k} x_i) \equiv 1 \mod m$. Hence the congruence $nx \equiv 1 \mod m$ has a solution, so again by the above fact $gcd(n, m) \mid 1$ which forces $gcd(n, m) = 1$.

(b) We argue by induction on k, with $k = 2$ being the base case. Suppose that $n_1 \mid m$ and $n_2 \mid m$ with $gcd(n_1, n_2) = 1$. Then $m = n_1 u$ for some $u \in \mathbb{Z}$ and $n_2 \mid n_1 u$. Since $gcd(n_1, n_2) = 1$, by the Coprime Lemma we get $n_2 \mid u$, so $u = n_2 v$ for some $v \in \mathbb{Z}$ and hence $m = n_1 n_2 v$, so $n_1 n_2 \mid m$.

Induction step: Now fix $k > 2$, and assume the assertion of (b) holds for $k - 1$. Consider the $k - 1$ integers $n_1 n_2, n_3, \ldots, n_k$. By part (a) $n_1 n_2$ is coprime to each n_i for $i \geq 3$, so these $k - 1$ integers are pairwise coprime. Also each of them divides m (where $n_1 n_2 \mid m$ by the base case and the rest divide m by assumption). Thus, we can apply the induction hypothesis to conclude that the product of those $k - 1$ integers (which is equal to n) also divides m.

2. Find the general solution for each of the following congruences:

(a) $8x \equiv 7 \mod 203$

(b) $14x \equiv 7 \mod 203$

(c) $14x \equiv 6 \mod 203$

Solution: (a) Using the ad hoc method and the first cancellation law (see Lecture 2), we get $8x \equiv 7 \mod 203 \iff 8x \equiv 210 \mod 203$

$\iff 4x \equiv 105 \mod 203 \iff 4x \equiv 308 \mod 203 \iff x \equiv 77 \mod 203$. So the general solution is $x = 77 + 203k$ with $k \in \mathbb{Z}$.

(b) Since 7 divides 14, 7 and 203, by the second cancellation law $14x \equiv 7 \mod 203 \iff 2x \equiv 1 \mod 29$. Since $2x \equiv 1 \mod 29 \iff 2x \equiv 30 \mod 29 \iff x \equiv 15 \mod 29$, the general solution is $x = 15 + 29k$ with $k \in \mathbb{Z}$.

(c) This congruence has no solutions since $gcd(14, 203) = 7$ does not divide 6.

3.

(a) Use the proof of CRT given in class to find a solution to the system of congruences

$$x \equiv a \mod 7, \quad x \equiv b \mod 11, \quad x \equiv c \mod 13,$$

where a, b and c are fixed (but unspecified) integers. Recall that first one needs to solve the system for the triples $(a, b, c) = (1, 0, 0)$, $(0, 1, 0)$ and $(0, 0, 1)$, after which one can write down a solution in the general case.

(b) Now use your answer in (a) to find the general solution to the system of congruences

$$x \equiv 3 \mod 7, \quad 2x \equiv 4 \mod 11, \quad 3x \equiv 5 \mod 13.$$

Solution: (a) We first find solutions x_1, x_2, x_3 corresponding to the triples $(a, b, c) = (1, 0, 0), (0, 1, 0)$ and $(0, 0, 1)$, respectively. Following the proof of CRT from class, this reduces to solving congruences $143z_1 \equiv 1 \mod 7$, $91z_2 \equiv 1 \mod 11$ and $77z_3 \equiv 1 \mod 13$. These simplify to $3z_1 \equiv 1 \mod 7$, $3z_2 \equiv 1 \mod 11$ and $-z_3 \equiv 1 \mod 13$. Solving these, we get that $z_1 = -2$, $z_2 = 4$ and $z_3 = -1$, so $x_1 = 143(-2) = -286$, $x_2 = 91 \cdot 4 = 364$ and $x_3 = 77 \cdot (-1) = -77$ are the desired solutions. Hence (again by the argument from the proof from class), given arbitrary $a, b, c \in \mathbb{Z}$, a particular solution to the system is $x = -286a + 364b - 77c$, and the general solution is $x = -286a + 364b - 77c + 1001k$ with $k \in \mathbb{Z}$ (since $7 \cdot 11 \cdot 13 = 1001$).

(b) Using the ad hoc method, we see that the system in (b) is equivalent to the following one:

$$x \equiv 3 \mod 7, \quad x \equiv 2 \mod 11, \quad x \equiv 6 \mod 13.$$

By (a) the general solution is $x = -286 \cdot 3 + 364 \cdot 2 - 77 \cdot 6 + 1001k = -592 + 1001k$ with $k \in \mathbb{Z}$. Replacing -592 by $-592 + 1001$, we can also write the general solution as $409 + 1001k$.

4. Find a solution to the congruence $25x \equiv 31 \mod 84$ using the method of Example 3.16.

Solution: Since $84 = 2^2 \cdot 3 \cdot 7$, the congruence $25x \equiv 31 \mod 84$ is equivalent to the system $25x \equiv 31 \mod 4$, $25x \equiv 31 \mod 3$ and $25x \equiv 31 \mod 7$ which simplify to $x \equiv 3 \mod 4$, $x \equiv 1 \mod 3$ and $4x \equiv 3 \mod 7$. Solving the latter system as in 3(b), we deduce that the general solution is $x = 55 + 84k$.

5.

(a) Let n be a positive integer. Prove that for any integer x there exists an integer r such that $x \equiv r \mod n$ and $0 \leq r \leq n-1$.
(b) Prove that $x^4 \equiv 0$ or $1 \mod 5$ for any integer x. **Hint:** using (a) one can solve the problem by simple case exhaustion.
(c) Prove that there exist no integers a and b such that $a^4 + b^4 = 20000000013$. **Hint:** the number of zeroes on the right hand side is completely irrelevant.

Solution: (a) This is clear from the division with remainder theorem (just let r be the remainder of dividing x by n).

(b) By (a) for any $x \in \mathbb{Z}$ there exists $r \in \{0,1,2,3,4\}$ such that $x \equiv r \mod 5$. Then $x^4 \equiv r^4 \mod 5$. Since $0^4 = 0$, $1^4 = 1$, $2^4 = 16 \equiv 1 \mod 5$, $3^4 = 81 \equiv 1 \mod 5$ and $4^4 = 256 \equiv 1 \mod 5$, the result follows.

(c) By (b) for any $a, b \in \mathbb{Z}$ the number a^4+b^4 is congruent to $0+0=0$, $0+1=1$ or $1+1=2 \mod 5$. Since $20000000013 \equiv 3 \mod 5$, the equation $a^4 + b^4 = 20000000013$ has no integer solutions.

7. Let p be a prime.

(a) Let $0 < k < p$ be an integer. Prove that $p \mid \binom{p}{k}$. **Hint:** First prove the following lemma: Suppose that $n, m \in \mathbb{Z}$, p is prime, $m \mid n$, $p \mid n$ and $p \nmid m$. Then $p \mid \frac{n}{m}$.
(b) Now prove that $(a+b)^p \equiv a^p + b^p \mod p$ for any integers a and b.
(c) Show by example that the assertions of (a) and (b) may become false without the assumption that p is prime.

Solution: (a) We first prove the lemma from the hint. Let $q = \frac{n}{m}$. Then $n = mq$, and by assumption $q \in \mathbb{Z}$. We are given that $p \mid n$, so $p \mid mq$. Since p is prime, by Euclid's lemma $p \mid m$ or $p \mid q$.

But we are given that $p \nmid m$. Therefore, $p \mid q$, that is, $p \mid \frac{n}{m}$. $\square$

Now we prove that $p \mid \binom{p}{k}$ for $0 < k < p$. Let $n = p!$ and $m = k!(p-k)!$, so that $\binom{p}{k} = \frac{n}{m}$. We will show that the above lemma applies to this triple (p, n, m).

First of all, $p \mid n$ since $p! = p \cdot (p-1)!$. By generalized Euclid's lemma $p \nmid k!(p-k)!$, since $k!(p-k)! = 1 \cdot \ldots \cdot k \cdot 1 \cdot \ldots \cdot (p-k)$, and all factors in the last product are less than p (hence not divisible by p). Finally, we know that $\frac{n}{m} \in \mathbb{Z}$ (e.g. by binomial theorem).

Thus, the lemma indeed applies, and we get $p \mid \frac{n}{m}$, that is, $p \mid \binom{p}{k}$.

(b) This follows directly from (a) and the binomial theorem (by (a) all the terms in the binomial expansion of $(a+b)^p$ except a^p and b^p are divisible by p).

(c) For instance 4 does not divide $\binom{4}{2} = 6$. Also $(1+1)^4 = 16$ is not congruent to $1^4 + 1^4 = 2 \bmod 4$.