Homework 3, solutions

Solution to problem 13. a) Since a is even, it can be written as $a = 2b$ for some integer b. Thus $a^2 = 4b^2$, so $4|a^2$, which is equivalent to $a^2 \equiv 0(\mod 4)$.

b) If a is odd then $a = 4b \pm 1$ for some integer b and some choice of the sign in ± 1 (i.e. either $a+1$ or $a-1$ is divisible by 4). Then

$$a^2 = 16b^2 \pm 8b + 1 = 8(2b^2 \pm 1) + 1.$$

It follows that $8|(a^2-1)$, i.e. $a^2 \equiv 1(\mod 8)$. Clearly this implies that $a^2 \equiv 1(\mod 4)$.

c) Consider a sum of two squares of integers $a^2 + b^2$. If both a and b are even then by a) we see that

$$a^2 + b^2 \equiv 0 + 0 = 0(\mod 4).$$

If both a and b are odd, then by b) we get

$$a^2 + b^2 \equiv 1 + 1 = 2(\mod 4).$$

Finally, if one of a, b is odd and the other is even then a) and b) imply that

$$a^2 + b^2 \equiv 1 + 0 = 1(\mod 4).$$

We see that a sum of two squares is never congruent to $3(\mod 4)$, i.e. a nuber $n \equiv 3(\mod 4)$ can not be expressed as a sum of two squares of integers.

Solution to problem 21. We have $(172195)(572167) = 985242x6565$. We will work modulo 11 and use what we learned in class (see problem 18 in the book). We have

$$172195 \equiv 5-9+1-2+7-1 = 1(\mod 11), \quad 572167 \equiv 7-6+1-2+7-5 = 2(\mod 11),$$

and

$$985242x6565 \equiv 5-6+5-6+x-2+4-2+5-8+9 = 4+x(\mod 11).$$

It follows that $4 + x \equiv 1 \cdot 2 = 2(\mod 11)$, i.e. $x \equiv -2(\mod 11)$. The only digit which satisfies this congruence is $x = 9$.

Solution to problem 26. a) The congruence $a^2 \equiv b^2 (\mod p)$ means that

$$p|(a^2 - b^2) = (a-b)(a+b).$$

Since p is a prime number, Euclid's Lemma tells us that either $p|(a-b)$ or $p|(a+b)$. The first case says $a \equiv b (\mod p)$, the second case says $a \equiv -b (\mod p)$. In other words, $a \equiv \pm b (\mod p)$.

b)We use same reasoning as in a). We have $p|(a^2 - a) = a(a-1)$, so either $p|a$ or $p|(a-1)$ (by Euclid's Lemma). Thus either $a \equiv 0 (\mod p)$ or $a \equiv 1 (\mod p)$.

Remark. The above argument easily extends to the following general result (equivalent to Euclid's Lemma):
if p is a prime and $ab \equiv 0 (\mod p)$ the either $a \equiv 0 (\mod p)$ or $b \equiv 0 (\mod p)$.

Solution to Problem 28e): We start by recalling the general method of solving a congruence of the form $ax \equiv b (\mod m)$. We first run Euclid's algeorithm to find $d = \gcd(a, m)$. If d does not divide b then there are no solutions to the congruence. If $d|b$ then we read from the Euclid's algorithm u, w such that $au + mw = d$. Let x be the reminder of ub/d upon division by m/d. Then the congruence has exactly d solutions give by the following list:

$$x, x + \frac{m}{d}, x + 2\frac{m}{d}, \ldots, x + (d-1)\frac{m}{d}.$$

We now solve the congruence $623x \equiv 511 (\mod 679)$. We start by finding the $d = \gcd(623, 679)$:

$$679 = 1 \cdot 623 + 56,\ 623 = 11 \cdot 56 + 7,\ 56 = 8 \cdot 7 + 0.$$

Thus $d = \gcd(679, 623) = 7$ and $7 = 12 \cdot 623 - 11 \cdot 679$. We take $u = 12$. Since $b/d = 511/7 = 73$ and $m/d = 679/7 = 97$ we get $ub/d = 12 \cdot 73 \equiv 3 (\mod 97)$. Thus the solutions modulo 679 to our original congruence are 3, $3 + 97 = 100$, $100 + 97 = 197$, $197 + 97 = 294$, $294 + 97 = 391$, $391 + 97 = 488$, $488 + 97 = 585$.

Part f) is solved by the same method.

Solution to Problem 29f: Recall thet when n, m are relatively prime then we can find s, t such that $sn + tm = 1$ (for example, using the Euclidean algorithm). Then we have $ns \equiv 1 (\mod m)$, so s is an inverse of n modulo m.

We do this when $n = 1333$, $m = 1517$. The Euclidean algorithm runs as follows:

$$1517 = 1\cdot 1333 + 184,\ 1333 = 7\cdot 184 + 45,\ 184 = 4\cdot 45 + 4,\ 45 = 11\cdot 4 + 1,\ 4 = 4\cdot 1 + 0.$$

From this we have $371 \cdot 1333 - 326 \cdot 1517 = 1$. Thus the inverse of 1333 modulo 1517 is 371.

Part e) is solved by the same method.

Problem 1. Let a, b, c be positive integers such that $\gcd(a, b) = 1$. We showed in class that if $c > ab$ then the equation $ax + by = c$ is solvable in positive integers x, y and that for $c = ab$ it does not have solutions in positive integers. Suppose now that $1 \leq c < ab$.

a) Show that if neither a nor b divides c then exactly one of the equations

$$ax + by = c, \quad ax + by = ab - c$$

has solutions in positive integers x, y.

b) If $c = am$ for some m the the only solution to $ax+by = c$ in non-negative integers is $x = m$, $y = 0$.

Solution. We recall first some observations from class. We proved that if $\gcd(a, b) = 1$ then for any integer c the equation $ax+by = c$ has solutions in integers. Moreover, if x_0, y_0 is one such solution then all solutions are given by $x = x_0 + kb$, $y = y_0 - kb$, where k is an integer. Solutions in positive integers correspond to integers k such that $x_0 + kb > 0$ and $y_0 - ka > 0$, i.e.

$$\frac{-x_0}{b} < k < \frac{y_0}{a}.$$

a) Let x_0, y_0 be a solution to $ax+by = c$ in integers, i.e. x_0, y_0 are integers such that $ax_0 + by_0 = c$. Then $a(-x_0) + b(a - y_0) = ab - ax_0 - by_0 = ab - c$, so $-x_0, a - y_0$ is a solution to $ax + by = ab - c$. By our discussion above, the equation $ax + by = c$ has solution in positive integers iff there is an integer between $-x_0/b$ and y_0/a. Similarly, $ax + by = ab - c$ has a solution in positive integers iff there is an integer between x_0/b and $(a - y_0)/a$. The last condition is equivalent to having an integer between $(y_0 - a)/a = -1 + y_0/a$ and $-x_0/b$. Since c is not divisible by a or b the numbers

x_0/b and y_0/a are not integers. There is exactly one integer between $-1+y_0/a$ and y_0/a and it is either between $-1+y_0/a$ and $-x_0/b$ or between $-x_0/b$ and y_0/a. Thus exactly one of the equations $ax+by=c$, $ax+by=ab-c$ has solution in positive integers (and such solution is unique).

b) If $c=am$ then $ax+by=c$ implies that a divides by. Since a and b are relatively prime, a divides y. If y is positive then $y \geq a$, so $by \geq ab > c$ so x must be negative. In other words, if x, y is a solution in non-negative integers, then $y=0$ and $x=m$.

Problem 2. John needs to pay \$2.05. He has only dimes and quarters. In how many ways he can pay?

Solution. The problem asks for solutions in non-negative integers x, y of the equation $10x+25y=205$. This is the same as solving $2x+5y=41$. Note that $\gcd(2,5)=1$. From Euclid's algorithm we see that $1=-2\cdot 2+1\cdot 5$. Thus $41=2\cdot(-82)+5\cdot 41$. All integer solutions to $2x+5y=41$ are given by $x=-82+5k$, $y=41-2k$, $k\in\mathbb{Z}$. To get non-negative solutions we need $-82+5k\geq 0$ and $41-2k\geq 0$, i.e.

$$\frac{82}{5}\leq k\leq \frac{41}{2}.$$

Now $82/5=16.4$ and $41/2=20.5$. Thus there are four possibilities for k: $17, 18, 19, 20$ which correspond to 4 different solutions:

$x=3, y=7$

$x=8, y=5$

$x=13, y=3$

$x=18, y=1$.

Problem 3. Let m, n be positive integers. How many multiples of n are in the sequence $m, 2m, 3m, \ldots, nm$?

Solution: The problem asks about the number of solutions to the congruence $mx\equiv 0(\mod n)$ among the numbers $1, 2, \ldots n$. Since the set $1, 2, \ldots n$ forms a complete system of residues modulo n, it is the same as to ask about the number of incongruent solutions modulo n to $mx\equiv 0(\mod n)$. Since $\gcd(m,n)$ clearly divides 0, we know that solutions exists and their numbers is exactly $\gcd(m,n)$. Thus there are exactly $\gcd(m,n)$ multiples of n in our sequence.

Problem 4. Find a positive integer such that half of it is a square, a third of it is a cube, and a fifth of it is a fifth power. Hint: Look for a number of the form $2^a 3^b 5^c$.

Solution: We recall first the following simple but very useful obsrevation: a positive integer n is a k-th power if and only if every prime number appears in n with exponenet divisible by k. In other words, n is a k-th power if and only if $e_p(n)$ is divisible by k for every prime number p.

We look for our number among numbers of the form $2^x 3^y 5^z$. Half of our number, i.e. $2^{x-1}3^y 5^z$ is a square if and only if $x-1$, y, z are all even. Similarly, a third of our number, i.e. $2^x 3^{y-1} 5^z$, is a cube if and only if all three numbers $x, y-1, z$ are divisible by 3. Finally, a fifth of our number, i.e. $2^x 3^y 5^{z-1}$, is a fifth power if and only if all three numbers $x, y, z-1$ are divisible by 5. Thus we are looking for a positive integer x which satisfies the following congruences:

$$x \equiv 1(\mod 2), \quad x \equiv 0(\mod 3) \quad x \equiv 0(\mod 5).$$

By the Chinese remainder theorem, there is unique such x modulo 30. Following the method provided by the Chinese remainder theorem we find that $x = 15$ works.

Similarly, we are looking for a positive integer y such that

$$y \equiv 0(\mod 2), \quad y \equiv 1(\mod 3) \quad y \equiv 0(\mod 5).$$

Again, using the Chinese remainder theorem, we find that $y = 10$ works.

Finally, we are looking for positive integer z such that

$$z \equiv 0(\mod 2), \quad z \equiv 0(\mod 3) \quad z \equiv 1(\mod 5).$$

The Chinese remainder theorem allows us to find that $z = 6$ works.

Thus the number $2^{15}3^{10}5^6$ satisfies the conditions of our problem.

Execise: Show that a number n is a sulution to the problem if and only if $n = 2^{15}3^{10}5^6 m^{30}$ for some integer m.