Homework 5, solutions

Problem 1. Let m, n be positive integers. How many multiples of n are in the sequence $m, 2m, 3m, \dots, nm$?

Solution: The problem asks about the number of solutions to the congruence $mx \equiv 0(\mod n)$ among the numbers $1, 2, \dots n$. Since the set $1, 2, \dots n$ 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 2. 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: think in terms of prime factorization.

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 $2^x3^y5^z$. Half of our number , i.e. $2^{x-1}3^y5^z$ is a square if and only if $x-1$, y, z are all even. Similarly, a third of our number, i.e. $2^x3^{y-1}5^z$, 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. $2^x3^y5^{z-1}$, 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 $n = 2^{15}3^{10}5^6m^{30}$ for some integer m.

Solution to Problem 38. Let $d = \gcd(m_1, m_2)$. If x is a solution to

$$x \equiv b_1(\mod m_1), \ \ x \equiv b_2(\mod m_2)$$

then x satisfies also the congruences

$$x \equiv b_1(\mod d), \quad x \equiv b_2(\mod d).$$

Subtracting the last two congruences, we get $b_1 - b_2 \equiv 0(\mod d)$, so indeed d must divide $b_1 - b_2$.

Suppose converesely, that d divides $b_1 - b_2$. We look for a solution x of the form $b_1 + ym_1$ for appropriate integer y. Any such integer automatically is a solution to the first congruence and in order to be a solution to the second congruence we must have $b_1 + ym_1 \equiv b_2(\mod m_2)$. This congruence is equivalent to

$$m_1 y \equiv b_2 - b_1(\mod m_2).$$

Since $\gcd(m_1, m_2) = d | b_2 - b_1$, we know that this congruence has a solution y and then $x = b_1 + m_1 y$ is a solution to our sytem of congruences.

Finally, suppose that x_1 and x_2 both are solutions to our system. Then

$$x_1 \equiv x_2 \equiv b_1(\mod m_1) \ \text{ and } \ x_1 \equiv x_2 \equiv b_2(\mod m_2).$$

It follows that both m_1 and m_2 divide $x_1 - x_2$, and threfore also the $\operatorname{lcm}(m_1, m_2)$ divies $x_1 - x_2$. This means that the solution is unique modulo $\operatorname{lcm}(m_1, m_2)$.

Solution to Problem 35: We want to find a smallest positive integer n such that

$$n \equiv 1(\mod 2), \ n \equiv 2(\mod 3), \ n \equiv 3(\mod 4),$$

$$n \equiv 4(\mod 5),\ n \equiv 5(\mod 6),\ n \equiv 0(\mod 7).$$

We can not apply the Chinese reminder theorem right away as the moduli are not pairwise relatively prime. We note however that some of the congruences are consequences of the others. In fact, suppose that n satisfies

$$n \equiv 2(\mod 3),\ n \equiv 3(\mod 4),\ n \equiv 4(\mod 5),\ n \equiv 0(\mod 7).$$

The second congruence tells us that n is odd, so $n \equiv 1(\mod 2)$. Also, as n is odd and $n \equiv 2(\mod 3)$, we have $n \equiv 5(\mod 6)$ (the system $x \equiv 1(\mod 2)$, $x \equiv 2(\mod 3)$ has a unique solution modulo 6, and 5 is that solution). So we reduced our problem to a sysstem of 4 congruences which satisfy the requirements of the Chinese remainder theorem, as the moduli $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, and $m_4 = 7$ are pairwise relatively prime. We have $b_1 = 2$, $b_2 = 3$, $b_3 = 4$, $b_4 = 0$.

To solve the system, we take $M = 3 \cdot 4 \cdot 5 \cdot 7 = 420$. Then $M_1 = 420/3 = 140$, $M_2 = 420/4 = 105$, $M_3 = 420/5 = 84$, $M_4 = 420/7 = 60$. Now we need to find the inverse x_i of M_i modulo m_i, $i = 1, 2, 3, 4$. Then

$$n \equiv M_1x_1b_1 + M_2x_2b_2 + M_3x_3b_3 + M_4x_4b_4(\mod M)$$

will be our solution. Finding the inverses is rather easy as the moduli m_i are small. As $M_1 \equiv 2(\mod 3)$, we see that $x_1 = 2$. Similarly, $M_2 \equiv 1(\mod 4)$, so $x_2 = 1$. Now $M_3 \equiv 4(\mod 5)$ so $x_3 = 4$. Finally $M_4 \equiv 4(\mod 7)$so $x_4 = 2$. It follows that

$$n \equiv 140 \cdot 2 \cdot 2 + 105 \cdot 1 \cdot 3 + 84 \cdot 4 \cdot 4 + 60 \cdot 2 \cdot 0 = 560 + 315 + 1404 \equiv 119(\mod 420).$$

The smallest positive solution is therefore 119

Solution to Probl;em 34c): We are asked to solve the system

$$5x \equiv 3(\mod 7),\ \ 2x \equiv 4(\mod 8)\ \ 3x \equiv 6(\mod 9).$$

This problem may be slighly confusing. When we deal with one congruence modulo some integre m then solving the congruence means finding all residues modulo m which satisfy the congreunce. In the above problem we have several congruences, with different moduli, so what do we mean by solving it? Well, one answer is that we want to describe all integers x which satisfy the system of congruences. We will do just that.

In the first congruence, 5 is relatively prime to 7, so it is invertible modulo 7 and the inverse of 5 modulo 7 is easily seen to be 3. Multiplying the congruence by 3, we get equivalent congruence $x \equiv 2(\mod 7)$. For the second congruence, note that x satisfies $2x \equiv 4(\mod 8)$ if and only if x satisfies $x \equiv 2(\mod 4)$. Finally, x satisfies the third congruence if and only if $x \equiv 2(\mod 3)$. Thus, the set of all integers satisfying our original system of congruences is the same as the set of integral solutions to the system

$$x \equiv 2(\mod 7), \quad x \equiv 2(\mod 4) \;\; x \equiv 2(\mod 3).$$

This system qualifies for the Chinese remainder theorem. Following the method provided by this theorem, we find that the unique solution modulo $3 \cdot 4 \cdot 7 = 84$ to this system is $x = 2$ (in this particular case the system is so simple that we do not need to involve the Chinese remainder theorem: we are looking for x such that $x - 2$ is divisible by 7, 4, and 3, which is the same as $x - 2$ divisible by 84). Thus the solutions to the system all all integers x such that $x \equiv 2(\mod 84)$.

Remark. The original problem could be phrased as follows: find all solutions modulo $7 \cdot 8 \cdot 9 = 504$ of the given system. In this case, the answer would be that there are 6 solutions modulo 504: $2, 86, 170, 254, 338, 422$.

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.

Solution to Problem 28e): We start by finding the $\gcd(623, 679)$:

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

Thus $\gcd(678, 623) = 7$ and $7 = 12 \cdot 623 - 11 \cdot 679$. Dividing by 7, we have

$$1 = 12 \cdot 89 - 11 \cdot 97.$$

Now $511 = 7 \cdot 73$, so the congruence has solutions and we will have 7 different solutions modulo 679. To find these solutions we first solve $89x \equiv 73(\mod 97)$. From our computations above we see that 12 is the inverse of 89 modulo 97. Thus $x \equiv 12\cdot 73 \equiv 3(\mod 97)$. Thus the solutions modulo 679 to our original congruence are 3, $3+97=100$, $100+97=197$, $197+97=294$, $294+97=391$, $391+97=488$, $488+97=585$.