Dr. Marques Sophie
Office 519

Number theory

Fall Semester 2013
marques@cims.nyu.edu

Problem Set #7

Due monday october 28th in Class

Exercise 1: ($\star\star$) 4 points
Obtain three consecutive integers, each having a square factor.
Solution:
The idea here is to set up the problem so that the Chinese Remainder Theorem applies. Let's call the first integer a. Note that if $2^2|a$, then a certainly has a square factor. The next integer also needs to have a square factor. The next integer also needs to have a square factor. It definitely will not have 2^2as factor; lets assume that 3^2 is the square factor of the next integer, $a+1$. Finally, we may assume that 5^2 is a factor of the last integer, $a+2$. So we have:

$$2^2|a, 3^2|a+1, 5^2|a+2$$

Translating these divisibility conditions into the language of congruences, we get:

$$a \equiv 0(mod\ 4),\ a \equiv -1(mod\ 9),\ a \equiv -2(mod\ 25)$$

But now to find a suitable a, we need only solve the above system of congruences using C.R.T. We can look for a particular solution of the two first congruence of the form $a = 4k + 9m$, this lead to $9m \equiv -m \equiv 0 mod 4$ and $4k \equiv -5k \equiv -1\ (mod\ 9)$ then $k = 2$ is a particular solution of the previous equation, then 8 is a particular solution of the two first equations; By C.R.T, we know that a general solution of this two equations of the form, $8 + 36l$, for some integer l. We want this solution to be also a solution of the last equation then we get $8 + 36l \equiv -2(mod\ 25)$, then $11l \equiv -10(mod\ 25)$. Since 0 is a solution of the equation $11l \equiv -10(mod\ 5)$, we can try to find a solution of the form $5j$ where j is an integer then we get $11j \equiv j \equiv -2(mod 5)$ then $l = -10$ is a particular solution of the equation $11l \equiv -10(mod\ 25)$. Finally $8 + 36 \times (-10) = -352$ is a particular solution of a the three equations. The three consecutive integer are then -350, -351, -352.

Exercise 2: ($\star$) 4 points
Show by induction that if n is a positive integer, then $4^n \equiv 1 + 3n(mod\ 9)$.
Solution:
For the base case $4 \equiv 1 + 3\ (mod\ 9)$. For the induction hypothesis, assume that $4^n \equiv 1 + 3n\ (mod 9)$ for some positive integer n. Then

$$4^n = 4.4^n \equiv 4(1 + 3n) \equiv 4 + 12n \equiv 4 + 3n \equiv 1 + 3(n + 1)\ (mod\ 9)$$

Therefore $4^n \equiv 1 + 3n\ (mod\ 9)$ for all positive integers n.

Exercise 3: ($\star$) 4 points
Determine which integers a, where $1 \leq a \leq 14$, have an inverse modulo 14, and find the inverse of each of these integers modulo 14.
Solution:
The numbers a with a inverse modulo 14 *are those for which* $(a, 14) = 1$, *that are* $1, 3, 5, 9, 11$ *and* 13. *The inverse of each of these integers modulo* 14 *is also in that list, since if* $ab \equiv 1$ *(mod m), then both a and b have an inverse modulo m. So we see that* $1^{-1} = 1$, $3^{-1} = 5$, $5^{-1} = 3$, $9^{-1} = 11$, $11^{-1} = 9$ *and* $13^{-1} = 13$.

Exercise 4: ($\star$) 4 points
Show that if p is an odd prime and a is a positive integer not divisible by p, then the congruence $x^2 \equiv a \ (mod\ p)$ has either no solution or exactly two incongruent solutions.
Solution:
If the congruence has no solutions, we are done, so suppose that it has at least one solution c. Then $c^2 \equiv a \ (mod\ p)$, *so also* $(-c)^2 \equiv a \ (mod\ p)$. *if* $c \equiv -c \ (mod\ p)$, *then* $2c \equiv 0 \ (mod\ p)$. *Since p is odd, this implies that* $p|c$. *But then* $a \equiv c^2 \equiv 0 \ (mod\ p)$. *This is a contradiction since* $p \nmid a$. *Therefore c and* $-c$ *are incongruent solutions. Now, suppose b is another solution. Then* $b^2 \equiv c^2 \ (mod\ p)$, *so* $(b+c)(b-c) \equiv b^2 - c^2 \equiv 0 \ (mod\ p)$. *Then either* $p|(b+c)$ *or* $p|(b-c)$, *so* $b \equiv \pm c \ (mod\ p)$. *Therefore there are exactly two incongruent solutions modulo p.*

Exercise 5: ($\star$) 4 points

1. Let a be an integer, u, v, n, m natural numbers. We assume that m and n are relatively prime, that $a^u \equiv 1 \ mod\ m$ and that $a^v \equiv 1 \ mod\ n$. Show that $a^{lcm(u,v)} \equiv 1 \ mod\ (mn)$.
2. Let a be an integer relatively prime to 63. Show that $a^{36} \equiv 1 \ mod\ 63$.
3. Using question (a), show that we can improve the result in (b), by proving that for any integer relatively prime to 63, $a^6 \equiv 1 \ mod\ 63$.

Solution:

1. *Since m and n are relatively prime, if* $x \equiv 1 \ mod\ m$ *and* $x \equiv 1 \ modmn$. *Apply this fact to* $x = a^{lcm(u,v)}$. *Since* $lcm(u, v)$ *is a multiple of u (respectively v) the congruence* $a^{lcm(u,v)} \equiv 1 \ mod\ m$ *(respectively* $a^{lcm(u,v)} \equiv 1 \ mod\ n$*) follows from assumption that* $a^u \equiv 1 \ mod\ m$ *(respectively* $a^v \equiv 1 \ mod\ n$*).*
2. *We see* $63 = 3^2 \times 7$ *so that* $\phi(63) = 3(3-1) \times 6 = 36$. *Since a is coprime to* 63 *we can apply Euler's theorem and get* $a^{36} \equiv 1 \ mod\ 63$.
3. *Again we use that* $63 = 3^2 \times 7$. *By Euler's theorem again, we have* $a^6 \equiv 1 \ mod\ 3^2$ *and* $a^6 \equiv 1 \ mod\ 7$. *Take* $m = 3^2$, $n = 7$ *and* $u = v = 6$ *in part* (a) *to see that* $a^6 \equiv 1 \ mod\ 63$.

[1]

[1] ($\star$) = easy , ($\star\star$)= medium, ($\star\star\star$)= challenge