

# MAT 311: Number Theory

## Spring 2008

### Solutions to Practice Midterm 1

- Any positive integer  $n$  of the form  $4k + 3$  has a prime factor of the same form.  
Note that every odd prime is of the form  $4k + 3$  or  $4k + 1$ . Since  $n$  is odd it must be a product of odd primes. If all such primes are of the form  $4k + 1$ , so is their product. Thus there has to be a prime factor of the form  $4k + 3$ .  $\square$
- Show that  $N = n^4 + 1$  is composite for every  $n > 1$ .  
This question is wrong, since for  $n = 2$ , we have  $N = 17$  which is prime.  $\square$
- If  $n$  is composite, show that  $N = (n - 1)! + 1$  is not a power of  $n$ .  
Suppose, for a contradiction, that  $N$  was a power of  $n$ . Since  $n$  is composite, it has a prime factor *strictly less* than  $n$ , say,  $p$ . Being a power of  $n$ ,  $N$  has to be divisible by  $p$ . But  $N = 1 \cdot 2 \cdots p \cdots (n - 1) + 1$  obviously cannot be divisible by  $p$ , because  $p$  divides the first term on the right hand side, but not the second (which is 1). This gives a contradiction.  $\square$
- Find the smallest positive integer that giving remainders 1,2,3,4,5 when divided by 3,5,7,9,11, respectively.  
First note that if a number gives the remainder 4 when divided by 9, then it will automatically give the remainder 1 when divided by 3. So the first condition is superfluous. Now, the number we are looking for is the minimum of all positive integers  $x$  satisfying:

$$\begin{aligned}x &\equiv 2 \pmod{5} \\x &\equiv 3 \pmod{7} \\x &\equiv 4 \pmod{9} \\x &\equiv 5 \pmod{11}.\end{aligned}$$

Since  $\gcd(5,7,9,11)=1$ , there is a unique solution for  $1 \leq x \leq 5 \cdot 7 \cdot 9 \cdot 11 = 3465$  by Chinese remainder theorem. Its not hard to guess what this number is: First two congruences imply that  $x \equiv 17 \pmod{35}$ . Last two congruences imply that  $x \equiv 45 \pmod{99}$ . Combining these two gives  $x \equiv 1732 \pmod{3465}$ . So the smallest such integer is  $x = 1732$ .  $\square$

- Prove that any integer  $n$  can be written of the form  $n = x^2 + y^2 - z^2$ .  
If  $n = 2k$ , set  $x = k, y = 1, z = (k - 1)$ . If  $n = 2k - 1$ , set  $x = k, y = 0, z = (k - 1)$ .  $\square$
- Find all rational points on the ellipse  $4x^2 + 3y^2 = 1$ .  
Pick a rational point on this curve:  $(1/2, 0)$ . The line thru this point with rational slope  $m$  is given by the equation  $y = mx - m/2$ . This line intersects the curve at  $x = ((3m^2/4) - 1)/(2 + 3m^2/2)$ . All the rational points are determined as  $m$  runs over rational points. Hence the set of rational points is:  $\{(((3m^2/4) - 1)/(2 + 3m^2/2), m(((3m^2/4) - 1)/(2 + 3m^2/2)) - m/2) : m \in \mathbb{Q}\}$ .  $\square$
- (a) Find all homomorphisms  $\mathbb{Z}_4 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$ .  
Since  $\mathbb{Z}_4$  is cyclic, the homomorphism is determined by the image of the generator, which is 1. In order such a function to be a homomorphism, the order of the image of 1 should be a divisor of 4, namely 1, 2, or 4. For each such element in the target group, we get a different homomorphism. By inspection, we see that  $o(0, 0) = 1$ ,  $o(1, 0) = 2$  and all other elements have order not equal to 1,2 or 4. So there are two homomorphisms  $\varphi_1, \varphi_2$  such that  $\varphi_1(1) = (0, 0)$  (which gives the trivial homomorphism), and  $\varphi_2(1) = (1, 0)$ .  $\square$   
(b) Find all homomorphism  $\mathbb{Z}_2 \rightarrow \mathbb{Z}_3^\times$ .  
Since  $\mathbb{Z}_3^\times$  is isomorphic to the group  $\mathbb{Z}_2$ , we are looking for homomorphism  $\mathbb{Z}_2 \rightarrow \mathbb{Z}_2$  (those are called *endomorphisms*). Again the homomorphism is determined by the image of the generator 1. It can either go to 1 or 2. So there are two homomorphisms  $\varphi_1, \varphi_2$  such that  $\varphi_1(1) = 1$  (which gives the trivial homomorphism) and  $\varphi_2(1) = 2$ .  $\square$
- Find all solutions of  $234x + 567y = 9$   
We use Euclidean Algorithm:  $567 = 2 \cdot 234 + 99$ ,  $234 = 2 \cdot 99 + 36$ ,  $99 = 2 \cdot 36 + 27$ ,  $36 = 1 \cdot 27 + 9$ ,  $27 = 3 \cdot 9$ . Thus,  $9 = 36 - 27 = 3 \cdot 36 - 99 = 3 \cdot 234 - 7 \cdot 99 = 17 \cdot 234 - 7 \cdot 567$ . Thus all the solutions are given by  $x = 17 + 63k$  and  $y = -7 - 26k$ ,  $k \in \mathbb{Z}$ .  $\square$