Dr. Marques Sophie
Office 519

Number theory

Fall Semester 2013

marques@cims.nyu.edu

Problem Set #2

Due monday 16 September in Class

Exercise 1: ($\star$)
Compute $\gcd(935, 1122)$ and $\gcd(1876, 4534)$ by using Euclidean algorithm.

Solution:
Euclidean algorithm equations are below:

$$\begin{aligned} 1122 &= 1 \cdot 935 + 187 \\ 935 &= 5 \cdot 187 + 0 \end{aligned}$$

Thus, $\gcd(935, 1122) = 187$. *Next,*

$$\begin{aligned} 4534 &= 2 \cdot 1876 + 782 \\ 1876 &= 2 \cdot 782 + 312 \\ 782 &= 2 \cdot 312 + 158 \\ 312 &= 1 \cdot 158 + 154 \\ 158 &= 1 \cdot 154 + 4 \\ 154 &= 38 \cdot 4 + 2 \\ 4 &= 2 \cdot 2 + 0 \end{aligned}$$

Thus, $\gcd(1876, 4534) = 2$.

Exercise 2: ($\star$)
Find two integers a and b such that $a \cdot 244 + b \cdot 313 = \gcd(244, 313)$.

Solution:
To solve our question, we need to apply Euclidean algorithm:

$$\begin{aligned} 313 &= 1 \cdot 244 + 69 \\ 244 &= 3 \cdot 69 + 37 \\ 69 &= 1 \cdot 37 + 32 \\ 37 &= 1 \cdot 32 + 5 \\ 32 &= 6 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

So, we can conclude that $\gcd(244, 313) = 1$. *Then, Euclidean algorithm equations performed backward are given by:*

$$\begin{aligned} 1 &= 1 \cdot 5 - 2 \cdot 2 = 1 \cdot 5 - 2(32 - 6 \cdot 5) \\ &= -2 \cdot 32 + 13 \cdot 5 = -2 \cdot 32 + 13(37 - 1 \cdot 32) \\ &= 13 \cdot 37 - 15 \cdot 32 = 13 \cdot 37 - 15(69 - 1 \cdot 37) \\ &= -15 \cdot 69 + 28 \cdot 37 = -15 \cdot 69 + 28(244 - 3 \cdot 69) \\ &= 28 \cdot 244 - 99 \cdot 69 = 28 \cdot 244 - 99(313 - 1 \cdot 244) \\ &= 127 \cdot 244 - 99 \cdot 313 \end{aligned}$$

Exercise 3: ($\star$)
Prove that if n is odd, then $n^2 - 1$ is divisible by 8.

Solution:
Let $n = 2k - 1$ *where* $k \in \mathbb{Z}$. *Then,* $n^2 - 1 = 4k(k-1)$. $k(k-1)$ *is a product of two consecutive numbers, so 2 divides* $k(k-1)$. *Hence, 8 divides* $4k(k-1)$.

Exercise 4: ($\star$)
Which of the following equations have integer solutions? (Justify your answer but do not find solutions.)

1. $51x - 7y = 88$
2. $11x - 66y = 0$
3. $33x + 44y = 1$

Solution:

1. $(51, 7) = 1$ *so this equation has solutions.*
2. $(11; 66) = 11$ *and* $11 | 0$ *so this equation has solutions.*
3. $(33, 44) = 11$ *and* $11 \nmid 1$ *so this equation has no solutions.*

Exercise 5: ($\star$)
Determine all the integer solutions of the equation:

$$4x + 7y = 117$$

Solution:
Compute the GCD of 4 and 7 :

$$(4,7) = 1 = 2 \times 4 + (-1) \times 7$$

You can also use the extended Gauss algorithm to find integers u and v such that

$$(4,7) = 2 \times u + 7 \times v$$

This give a particular solution for the initial system given by: $x_0 = 2 \times 117 = 234$
$y_0 = -1 \times 117 = -117$
Let (x, y) *be a general solution, we have then:*

$$4x + 7y = 117 = 4x_0 + 7y_0$$

Then

$$4(x - x_0) = 7(y - y_0)$$

Since $(4,7) = 1$ *then by Euclid's lemma, since* 4 *divides* $7(y - y_0)$, 4 *divides* $(y - y_0)$. *So, there is an integer* k *such that* $y - y_0 = 4k$. *Injecting this equation to the later one, we obtain* $x - x_0 = 7k$. *So, a general solution is of the form*

$$\begin{cases} x = 7k + 234 \\ y = 4k - 117 \end{cases}$$

We want $x \geq 0$ *and* $y \geq 0$, *then* $-234/7 \leq k \leq 117/4$ *There* 4 *such integers* k, *namely* k 33, 32, 31, 30.

Exercise 6 ($\star\star$):
A positive integer m has the prime decomposition $2^4 p_1 p_2 p_3$, where p_1, p_2, p_3 are some odd prime number (not necessarily distinct). The integer $m+100$ has the prime decomposition $5q_1q_2q_3$ where q_1, q_2, q_3 are som prime number different from 5 (not necessarily distinct). The integer $m + 200$ has the prime decomposition $23r_1r_2r_3r_4$, where r_1, r_2, r_3, r_4 are some prime number different from 23 (not necessarily distinct). Find m.
Solution:
The prime decomposition of 100 *is* $2^2 \times 5^2$. *Since the numbers* $m + 100$ *and* 100 *are divisible by* 5, *so their difference* m *and their sum* $m + 200$ *and then* 5 *appear in both decomposition.*
The prime decomposition of 200 *is* $2^3 \times 5^2$ *and* m *is divisible by* 2^3. *Then* $m + 200$ *is also divisible by* 2^3. *So we get the decomposition of* $m + 200$ *as* $2^3 \times 5 \times 23 = 920$. *And* $m = 920 - 200 = 720 = 2^4 \times 3^2 \times 5$. *(Remarque:* $m + 100 = 820 = 2^2 \times 5 \times 41$*).*
Exercice 7 ($\star$):
Is 211 prime? (Give a justification to your answer).
Solution:
We check whether 211 *is divisible by any prime less than* $\sqrt{211}$ *which is approximatively* $14,5$. *The primes smaller than* 14 *are* 2, 3, 5, 7, 11 *and* 13. *No one of them divides* 211 *so* 211 *is prime.* [1]

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