HOMEWORK 6 SOLUTIONS,
MS-A0402, FOUNDATIONS OF DISCRETE MATHEMATICS

2023

Homework

The written solutions to the homework problems should be handed in on MyCourses by Monday 17.4., 10:00. You are allowed and encouraged to discuss the exercises with your fellow students, but everyone should write down their own solutions.

Problem 1. (10pts) Does the following Diophantine equation

$$20x + 10y = 65.$$

have solutions $x, y \in \mathbb{N}$? If yes, find all the solutions. If not, justify your answer.

Solution 1. We compute

$$\gcd(20, 10) = \gcd(20 - 10, 10) = \gcd(10, 10) = \gcd(10 - 10, 10) = \gcd(0, 10) = 10$$

by the Euclidean algorithm. As 10 does not divide 65, the equation has no integer solutions.

Problem 2. (10pts) Does the following Diophantine equation

$$20x + 16y = 500.$$

have solutions $x, y \in \mathbb{N}$? If yes, find all the solutions. If not, justify your answer.

Solution 2. We compute $\gcd(20, 16)$ using the Euclidean algorithm.

$$\gcd(20, 16) = \gcd(20 - 1 \cdot 16, 16) = \gcd(4, 16) = \gcd(4, 16 - 4 \cdot 4) = \gcd(4, 0) = 4$$

Clearly 4 divides 500 so we expect the equation to have integer solutions. We can use the steps of the algorithm to write $500 = 125 \cdot 4$ as a linear combination of 20 and 16.

$$500 = 125 \cdot 4 = 125 \cdot (20 - 1 \cdot 16) = 20 \cdot 125 + 16 \cdot (-125)$$

So a particular solution is $x_0 = 125$ and $y_0 = -125$. Let $u = x - x_0$ and $v = y - y_0$ (x and y are some solution of the original equation). Then we must have the following.

$$20u + 16v = 0$$

This is a homogeneous Diophantine equation with solutions of the form $u = \frac{16}{4}k = 4k$ and $v = -\frac{20}{4}k = -5k$ with $k \in \mathbf{Z}$. We hence get that $x = u + x_0 = 4k + 125$ and $y = v + y_0 = -5k - 125$. Finally, we want only solutions such that $x, y \in \mathbb{N}$ so we get restrictions for k from $4k + 125 \geq 0$ and $-5k - 125 \geq 0$. Getting bounds for k from each inequality and combining these gives $-31.25 \leq k - 25$, meaning $-31 \leq k \leq -25$ as $k \in \mathbb{Z}$. The set of possible solution pairs (x, y) is hence

$$\{(4k + 125, -5k - 125) : k \in \mathbb{Z},\ -31 \leq k \leq -25\}.$$

Problem 3. (10pts) How many integers less than 22220 are relatively prime to 22220?

Solution 3. We note that $22220 = 10 \cdot 2222 = 2 \cdot 5 \cdot 2 \cdot 1111 = 2^2 \cdot 5 \cdot 11 \cdot 101$. As these are prime numbers and the prime factorization is always unique we can use Euler's totient function, which gives as the amount of relative primes

$$\phi(22220) = 22220 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{11}\right)\left(1 - \frac{1}{101}\right) = 8000.$$

Problem 4 What are the last two digits of 2023^{2023}?

Solution 4

Method 1

This is the same as finding $2023^{2023} \mod 100$. First note that

$$2023^{2023} \equiv 23^{2023} \mod 100$$

Let's find an m such that $23^m \equiv 1 \mod 100$. For this to be true we need the last digit to be 1. The last digit is determined by the last digit of the powers of 3, and these are $3, 9, 7, 1, 3, \ldots$. Note that it goes in a cycle of length 4. So to get a 1 we need $m = 4k$.

Now

$$23^{4k} = (23^4)^k \equiv (41)^k \mod 100$$

where $23^4 \mod 100$ is computed by brute force. Using the binomial expansion we have

$$(40+1)^k = 40^k + \cdots + \binom{k}{2} 40^2 + \binom{k}{1} 40 + 1 \equiv 40k + 1 \mod 100$$

because every term apart from the last two are multiples of 100.

We need to solve $40k + 1 \equiv 1 \mod 100$. The smallest value is $k = 5$. So $m = 20$. In conclusion $23^{20} \equiv 1 \mod 100$. Using this we have

$$23^{2023} = 23^{2020} 23^{23} = (23^{20})^{101} 23^3 \equiv (1)(23^3) \mod 100$$

By a brute force computation (already done above when we computed 23^4) we find that (23^3) mod $100 \equiv 67$. And this is the answer to our initial question.

Method 2 (outline only)

In this method we use Euler's formula. In some cases this is easier but in this particular example it does not help too much. First we computer Euler's phi function.

$$\phi(100) = \phi(2^2 \cdot 5^2) = 2 \cdot 1 \cdot 5 \cdot 4 = 40$$

Since 23 is prime, 23 and 100 are coprime and Eurler's theorem implies that

$$23^{40} \equiv 1 \mod 100$$

So

$$23^{2023} = 23^{2000} 23^2 3 = (23^{40})^{50} 23^{23} \equiv 1^{50} * 23^{23} \text{ mod } 100 \equiv 23^{23} \text{ mod } 100$$

But now what? One option is to write $23 = 20 + 3$ and use a binomial expansion as above. The remaining calculations are large but can be done on a calculator. Eventually this gives then answer as $40 + 27 = 67$. Another option is to break down the number using 23 = 2*11 + 1.

Another method is to look at $23^{40} \equiv 1 \text{ mod } 100$ which is of the form $x^2 \equiv a \text{ mod } n$. This is called a quadratic residue which is an important concept in number theory but is not something we have time for in this course.