

Solving discrete problems — Math 2020

Preparation for second lecture, January 20 2005

The course will start with an introduction to number theory, this will start with prime numbers and factorization, and end up with cryptography.

You should already know what a prime number is, and you should know about the following concepts, though you might not know their names. The best approach to the following questions is to try to work through them all without using the book, and only refer to the book after trying the questions.

A1. Integers: The set of integers is the set of whole numbers, $0, 1, 2, 3, \dots, -1, -2, \dots$

Later on we'll come back to section 3.2 and 3.3 and give a more rigorous definition.

Q2. Multiple: 90 is a multiple of 3, but not a multiple of 7.

What is the definition of a multiple of a positive integer?

Q3. Divisor or Factor: 8 is a factor of 80. What are all the factors of 15?

What is the definition of a factor of a positive integer? (A factor is the same thing as a divisor.)

We write $a|b$ to mean “ a divides b ”.

Q4. Remainders and Quotients: 8 goes into 60 7 times (7 is the quotient), with remainder 4.

In your own words, what does it mean to say that b goes into a q times with remainder r ?

(Note that a, b, q and r are all assumed to be integers.)

Given a and b , describe an algorithm (list of “steps”) for finding q and r .

Q5. Primes and composites: 3, 5 and 7 are primes.

If a positive integer is not prime it's called “composite”. What is the definition of a prime?

Is 541 a prime? What's the smallest prime which is greater than 600?

Q6. Relatively prime:

6 and 35 are not prime, but they are “relatively prime” – what does this mean?

Q7. Prime factorisation: The prime factorisation of 123456 is (in four different notations)

$$123456 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 3 \times 643 = 2^6 \times 3 \times 643 = 2^6 \cdot 3 \cdot 643 = 2^6 3^1 643^1.$$

What does it mean in general to find the prime factorisation of an integer?

Can a positive integer have more than one prime factorisation? Why, or why not?

Q8. Common Multiple and Least Common Multiple:

60 is a common multiple of 4 and 6. The least common multiple of 4 and 6 is 12. We'll write $\text{lcm}(4, 6) = 12$.

What is the definition of a common multiple and least common multiple of two positive integers?

Describe an algorithm for finding all possible pairs of positive integers a and b with $\text{lcm}(a, b) = 60$.

Q9. Common Divisor and Greatest Common Divisor:

2 is a common divisor of 20 and 30, and 10 is the greatest common divisor. We write $\text{gcd}(20, 30) = 10$.

What is the definition of common divisor and greatest common divisor of two positive integers?

If two positive integers are relatively prime, what is their gcd?

Given two positive integers, a and b , describe how you would find their greatest common divisor.

You can find the answers to all the above questions by reading through sections 3.4 and 3.5, pages 119 — 129 in the text book. But try to answer without looking at the book first. If you don't have the text book, you should be able to find the answers in any basic number theory book, or by searching on the web. One useful place to look for definitions is: <http://mathworld.wolfram.com/>

For this topic, see especially: <http://mathworld.wolfram.com/topics/Divisors.html>

and <http://mathworld.wolfram.com/topics/PrimeNumbers.html>

Next lecture:

1: After making sure we know all the above basic concepts, I want to discuss a particularly interesting kind of prime, called a “**Mersenne prime**”. This is also related to “perfect numbers”. If you want to think about these in advance, see: <http://mathworld.wolfram.com/MersennePrime.html>

2: Learning contracts.

I want to set up a learning contract for this course. Probably the main method of assessment will be an oral exam, based on a take home written exam. However, we will discuss the details next time.

There's a web page about learning contracts at: <http://www-distance.syr.edu/contract.html>