Worksheet on Number Theory

Benjamin Cosman, Patrick Lin and Mahesh Viswanathan

Fall 2020

Takeaways from Lecture

- $a \mid b$ means there exists an integer k such that $b = ak$. We say that a is a *factor* or *divisor* of b, and b is a *multiple* of a.
- For integers a and b with $a > 0$, there exist unique integers q, r such that $b = qa + r$ and $0 \leq r < a$. $q = \mathsf{quot}(b, a)$ is called the *quotient* and $r = \mathsf{rem}(b, a)$ is called the *remainder*.
- A number greater than 1 is *prime* if its only factors are 1 and itself. Every integer can be written as a product of a unique weakly decreasing sequence of primes.
- $\gcd(a, b)$ is the largest integer dividing both a and b. a and b are *coprime* if $\gcd(a, b) = 1$.
- $a \equiv b \bmod n$ means $n \mid (a - b)$. This equivalence relation splits the integers into *congruence classes* $[a]_n = \{b \mid a \equiv b \bmod n\}$. Any element $b \in [a]_n$ is called a *representative* of the congruence class; the *canonical representative* of $[a]_n$ is $\mathsf{rem}(a, n)$.
- Congruence classes can be added and multiplied.

Problem 1 (Quick computations/sanity checks)**.**

a) Compute $\mathsf{quot}(-22, 5)$ and $\mathsf{rem}(-22, 5)$.

b) Suppose $k = \gcd(a, b)$. What is $\gcd(-a, b)$, in terms of k?

c) Give an example of distinct integers a, b, c such that $\gcd(a, b) = 1$ and $\gcd(b, c) = 1$ but $\gcd(a, c) \neq 1$.

d) What is the number of congruence classes modulo n? What are their canonical representatives?

e) What is $\gcd(n, 0)$?

f) True or false: $-3 \mid 0$.

g) True or false: $0 \mid 3$.

h) True or false: If $\gcd(a, b) \mid c$ then $a \mid c$

i) True or false: If $c \mid \gcd(a, b)$ then $c \mid a$.

Problem 2. This problem is about the *Euclidean algorithm* for computing the gcd of two positive integers, which is presented below in pseudocode:

Euclidean algorithm

```
gcd(a,b): // a > b > 0
  x = a
  y = b
  while y > 0:
    r = rem(x,y)
    x = y
    y = r
  return x
```

a) Compute $\gcd(462, 210)$ using the Euclidean algorithm. Also compute the prime factorizations of 462 and 210, and use them to verify that the answer is correct.[1]

b) Prove that for all positive integers a, b, $\gcd(a, b) = \gcd(b, \mathsf{rem}(a, b))$.

   Hint: show that if n is a common factor of two of $a, b, \mathsf{rem}(a, b)$, then it is also a factor of the third.

c) Prove (via induction) that at the end of every iteration of the while loop, $\gcd(a, b) = \gcd(x, y)$.[2]

Problem 3. In the lecture, we saw that we can always perform modular arithmetic using the *canonical* representatives to simplify our calculations, especially computations of large powers modulo some n. Use this idea to perform the following computations. All of your answers should be written in terms of canonical representatives.

a) Compute $[7]_{11}^2$ $(= [7]_{11}[7]_{11})$.

b) Compute $[7]_{11}^4$. *Hint: Use part a.*

c) Compute $[7]_{11}^8$. *Hint: Use part b.*

d) Compute $[7]_{11}^{14}$. *Hint: Use parts a-c.*

e) Compute $[5]_{11}^5 + [7]_{11}^{14}$.

Problem 4. For integers a and b, if $a = b$, then $a - b = 0$, so for all integers n, $n \mid (a - b)$, i.e., $a \equiv b \bmod n$, or, equivalently, $[a]_n = [b]_n$.[3] In this problem, we use this idea to prove that certain equations have no integer solutions.[4]

a) Compute all congruence classes of perfect squares modulo 4. In other words, compute $[0^2]_4$, $[1^2]_4$, $[2^2]_4$, etc. How many distinct classes are there?

[1] You will probably find that computing $\gcd(462, 210)$ is much easier than finding the prime factorizations of 462 and 210. In general, computing prime factorizations is a much harder problem than computing gcds.

[2] This also serves as a proof that the algorithm is correct, since $x = \gcd(x, 0)$.

[3] People familiar with abstract algebra may recognize the mapping $a \mapsto [a]_n$ as an example of a *ring homomorphism*.

[4] You may have heard of the famous Fermat's Last Theorem, which states that for $n > 2$, there are no integer solutions to the equation $x^n + y^n = z^n$ (other than $x = y = z = 0$). The case of $n = 3$ took many decades and the invention of very sophisticated methods to prove, but it turns out that the case of $n = 4$ can be proven using this (comparatively) very simple technique!

b) Show that there are no integer solutions to the equation $x^2 + y^2 = 4003$.

Hint: use part (a) and the contrapositive of the statement $a = b \to [a]_n = [b]_n$.