Number Theory: The queen of mathematics*

MATH 231

1 Division and remainders

For any integer a and positive integer d there exists integers q and $0 \leq r < d$ such that

$$a = dq + r \tag{1}$$

and q and r are uniquely determined (i.e. once given a and d there is only one possibility for q and r).

Problem 1.

1. For $a = 23$ and $d = 7$ find the q and r in Equation (1).
2. For $a = 42$ and $d = 7$ find the q and r in Equation (1).
3. For $a = -12$ and $d = 7$ find the q and r in Equation (1).

Note we choose the letter r for "remainder" as we are exactly doing (long) division with remainder[1]. We say d *divides* a, and denote this $d \mid a$, if and only if $r = 0$ in Equation (1). This means $d \mid a$ if and only if there exists an integer q so that $a = dq$. In this case we see d is a *divisor* of a.

Problem 2.

1. Prove if $d \mid a$ and $d \mid b$, then $d \mid (a + b)$.
2. Prove if $d \mid m$ and $m \mid n$, then $d \mid n$.

2 Prime numbers

An integer $p > 1$ is called *prime* if $d \mid p$ implies that $d = 1$ or $d = p$. That is, a prime integer p has exactly two[2] divisors namely 1 and p. An integer $n > 1$ which is not prime is called *composite*. The integer n is composite if and only if $d \mid n$ for some $1 < d < n$ if and only if $n = qd$ for some $1 < d < n$. The following is a fundamental fact about prime numbers.

Lemma (Euclid's Lemma[3])**.** *Let p, a, and b be positive integers with p a prime integer. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Problem 3. Find a counterexample to a version of Euclid's Lemma where p is not required to be prime. That is, find a counter example to: "Let n, a, and b be positive integers. If $n \mid ab$, then $n \mid a$ or $n \mid b$."

Here is an important theorem to be aware of when dealing with prime numbers. Notice the statement has two conclusions: First, there exists a product of primes, and secondly the primes in the product are uniquely determined.

Theorem (Fundamental Theorem of Arithmetic)**.** *Every integer greater than 1 can be represented at a product of prime numbers in a way which is unique up to the order of the factors.*

*According to quote of Carl Friedrich Gauss.

[1]The r is the remainder you get from % and q is the "integer quotient" you get doing // in some programming languages.

[2]Here we have $p > 1$; so, p and 1 are different. Thus 1 is not a prime number.

[3]From Euclid's Elements circa 300 BC.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	60
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Figure 1: For you to find all prime numbers up to 100.

Problem 4. Find the representation as a product of primes from the Fundamental Theorem of Arithmetic for $n = 100$ and $n = 144$.

Say we want to prove $P(n)$ for all $n \geq C$. With *strong induction* we check $P(C)$ as a base case[4], then for some $n \geq C$ we assume $P(m)$ for all $m \leq n$. Then we show $(\forall m \leq n, P(m)) \to P(n+1)$. In other words, we assume *all* smaller cases to show next case. Whereas in the induction we encountered before only the single case directly prior was used to show the next case.

Problem 5. Use strong induction to show that every integer $n > 1$ can be written as the product of primes. (This is the Fundamental Theorem of Arithmetic without the uniqueness.)

3 Primality testing

Testing if a number is prime is an important computational task (e.g. used cryptography). One place that mathematics and theorem proving is useful is in making computational tasks more efficient. At first glance to test of an integer $n > 1$ is prime we have to check $n - 2$ things. We have to check if d divides n for each $1 < d < n$. However, we can do much better. We can reduce to checking only about $\sqrt{n}$ things.

Problem 6. Prove that if $n > 1$ is a composite number, then $d \mid n$ for some $1 < d \leq \sqrt{n}$.

Problem 7. Is it true that if $1 < n \leq 100$ and d does not divide n for all $2 \leq d \leq 10$, then n is prime?

Problem 8. Let us find all prime numbers less than or equal to 100 using an ancient method know as the sieve of Eratosthenes[5]. Use the grid of numbers in Figure 1. Start by circling 2 (because it's prime) then crossing out all multiples of 2 (they are composite). Circle the smallest remaining number which isn't circled or crossed (it should be 3) and then cross out all of it's multiples. Repeat as needed (the previous problem tells you when you can stop).

[4]Sometimes we have multiple base cases, but we won't need that presently.

[5]Eratosthenes (b. 276 BC) in additional to being a number theorist was the chief librarian at the Library of Alexandria, knew the Earth was not flat, and gave a very accurate measurement of the Earth's circumference.