Integers and Division

Why prime numbers?

- Prime numbers are not well understood
- Basis for today's cryptography
- Unless otherwise indicated, we are only talking about positive integers for this chapter

The divides operator

- New notation: 3 | 12
  - To specify when an integer evenly divides another integer
  - Read as “3 divides 12”
- The not-divides operator: 5 ∤ 12
  - To specify when an integer does *not* evenly divide another integer
  - Read as “5 does not divide 12”

Theorem on the divides operator

- If a | b and a | c, then a | (b+c)
  - Example: if 5 | 25 and 5 | 30, then 5 | (25+30)
- If a | b, then a | bc for all integers c
  - Example: if 5 | 25, then 5 | 25*c for all ints c
- If a | b and b | c, then a | c
  - Example: if 5 | 25 and 25 | 100, then 5 | 100

Prime numbers

- A positive integer p is prime if the only positive factors of p are 1 and p
  - If there are other factors, it is composite
  - Note that 1 is not prime!
    - It's not composite either – it's in its own class

- An integer n is composite if and only if there exists an integer a such that $a \mid n$ and $1 < a < n$

Fundamental theorem of arithmetic

- Every positive integer greater than 1 can be uniquely written as a prime or as the product of two or more primes where the prime factors are written in order of non-decreasing size

- Examples
  - 100 = 2 * 2 * 5 * 5
  - 182 = 2 * 7 * 13
  - 29820 = 2 * 2 * 3 * 5 * 7 * 71

Composite factors

- If n is a composite integer, then n has a prime divisor less than or equal to the square root of n

- Strong inductive proof using the following logic:
  - Since n is composite, it has a factor a such that $1<a<n$
  - Thus, $n = ab$, where a and b are positive integers greater than 1
  - Either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ (Otherwise, $ab > \sqrt{n} * \sqrt{n} > n$)

Showing a number is prime

- Show that 113 is prime

- Solution
  - The only prime factors less than $\sqrt{113} = 10.63$ are 2, 3, 5, and 7
  - Neither of these divide 113 evenly
  - Thus, by the fundamental theorem of arithmetic, 113 must be prime

Showing a number is composite

- Show that 899 is prime

- Solution
  - Divide 899 by successively larger primes (up to $\sqrt{899} = 29.98$), starting with 2
  - We find that 29 and 31 divide 899

- On a unix system, enter “factor 899”

```
aaron@orion:~.16> factor 899
899: 29 31
```

Primes are infinite

- Theorem (by Euclid): There are infinitely many prime numbers

- Proof by contradiction
- Assume there are a finite number of primes
- List them as follows: $p_1, p_2 \ldots, p_n$.
- Consider the number $q = p_1 p_2 \ldots p_n + 1$
  - This number is not divisible by any of the listed primes
    - If we divided p_i into q, there would result a remainder of 1
  - We must conclude that q is a prime number,

The prime number theorem

- The radio of the number of primes not exceeding x and $x/\ln(x)$ approaches 1 as x grows without bound
  - Rephrased: the number of prime numbers less than x is approximately $x/\ln(x)$
  - Rephrased: the chance of an number x being a prime number is
    $1 / \ln(x)$

- Consider 200 digit prime numbers

Showing a number is prime or not

- Consider showing that $2^{650}-1$ is prime
  - That number has about 200 digits
- There are approximately 10^{193} prime numbers less than $2^{650}-1$
  - By theorem 5 ($x/\ln(x)$, where $x = 2^{650}-1$)
- How long would that take to test each of those prime numbers?
  - Assume a computer can do 1 billion (10^9) per second
  - It would take $10^{193}/10^9 = 10^{184}$ seconds

The division “algorithm”

- Let a be an integer and d be a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq+r$

- We then define two operators:
  - $q = a$ **div** d
  - $r = a$ **mod** d

Greatest common divisor

- The greatest common divisor of two integers *a* and *b* is the largest integer *d* such that *d* | a and *d* | b
  - Denoted by gcd(a,b)

- Examples
  - gcd (24, 36) = 12
  - gcd (17, 22) = 1
  - gcd (100, 17) = 1

Relative primes

- Two numbers are *relatively prime* if they don't have any common factors (other than 1)
  - Rephrased: *a* and *b* are relatively prime if gcd (a,b) = 1

- gcd (25, 39) = 1, so 25 and 39 are relatively prime

More on gcd's

- Given two numbers *a* and *b*, rewrite them as: $a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$
  - Example: gcd (120, 500)
    - $120 = 2^3*3*5 = 2^3*3^1*5^1$
    - $500 = 2^2*5^3 = 2^2*3^0*5^3$
- Then compute the gcd by the following formula: $gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \ldots p_n^{\min(a_n,b_n)}$

Least common multiple

- The least common multiple of the positive integers *a* and *b* is the smallest positive integer that is divisible by both *a* and *b*.
  - Denoted by lcm (*a*, *b*)
  - $\mathrm{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \ldots p_n^{\max(a_n,b_n)}$
- Example: lcm(10, 25) = 50
- What is lcm (95256, 432)?
  - $95256 = 2^3 3^5 7^2$, $432 = 2^4 3^3$
  - lcm $(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,4)} 3^{\max(5,3)} 7^{\max(2,0)} = 2^4 3^5 7^2 = 190512$

lcm and gcd theorem

- Let *a* and *b* be positive integers. Then *a*b* = gcd(*a*,*b*) * lcm (*a*, *b*)

- Example: gcd (10,25) = 5, lcm (10,25) = 50
  - 10*25 = 5*50

- Example: gcd (95256, 432) = 216, lcm (95256, 432) = 190512
  - 95256*432 = 216*190512

Pseudorandom numbers

- Computers cannot generate truly random numbers!

- Algorithm for “random” numbers: choose 4 integers
  - Seed x_0: starting value
  - Modulus m: maximum possible value
  - Multiplier a: such that $2 \leq a < m$
  - Increment c: between 0 and m

Pseudorandom numbers

- Formula: $x_{n+1} = (ax_n + c) \bmod m$
- Let $x_0 = 3$, $m = 9$, $a = 7$, and $c = 4$

- $x_1 = 7x_0+4 = 7*3+4 = 25 \bmod 9 = 7$
- $x_2 = 7x_1+4 = 7*7+4 = 53 \bmod 9 = 8$
- $x_3 = 7x_2+4 = 7*8+4 = 60 \bmod 9 = 6$
- $x_4 = 7x_3+4 = 7*6+4 = 46 \bmod 9 = 1$
- $x_5 = 7x_4+4 = 7*1+4 = 46 \bmod 9 = 2$
- $x_6 = 7x_5+4 = 7*2+4 = 46 \bmod 9 = 0$

Pseudorandom numbers

- Formula: $x_{n+1} = (ax_n + c) \bmod m$
- Let $x_0 = 3$, $m = 9$, $a = 7$, and $c = 4$

- This sequence generates:
  3, 7, 8, 6, 1, 2, 0, 4, 5, 3 , 7, 8, 6, 1, 2, 0, 4, 5, 3
  - Note that it repeats!
  - But it selects all the possible numbers before doing so

The Caesar cipher

- Julius Caesar used this to encrypt messages

- A function f to encrypt a letter is defined as:
  $f(p) = (p+3) \bmod 26$
  - Where p is a letter (0 is A, 1 is B, 25 is Z, etc.)

- Decryption: $f^{-1}(p) = (p-3) \bmod 26$

- This is called a substitution cipher

The Caesar cipher

- Encrypt “go cavaliers”
  - Translate to numbers: g = 6, o = 14, etc.
    - Full sequence: 6, 14, 2, 0, 21, 0, 11, 8, 4, 17, 18
  - Apply the cipher to each number: $f(6) = 9$, $f(14) = 17$, etc.
    - Full sequence: 9, 17, 5, 3, 24, 3, 14, 11, 7, 20, 21
  - Convert the numbers back to letters 9 = j, 17 = r, etc.
    - Full sequence: jr wfdydolhuv

- Decrypt “jr wfdydolhuv”
  - Translate to numbers: j = 9, r = 17, etc.
    - Full sequence: 9, 17, 5, 3, 24, 3, 14, 11, 7, 20, 21
  - Apply the cipher to each number: $f^{-1}(9) = 6$, f

Rot13 encoding

- A Caesar cipher, but translates letters by 13 instead of 3
  - Then, apply the same function to decrypt it, as 13+13=26
- Rot13 stands for “rotate by 13”
- Example:

```
aaron@gemini:~.98> echo darth vader is luke skywalkers father | rot13
qnegu inqre vf yhxr fxljnyxref sngure
aaron@gemini:~.99> echo qnegu inqre vf yhxr fxljnyxref sngure | rot13
```