



Math

Ch. 3.4-3.6 Rosen

Numbers

Hello
World



Chapter Preview

In this chapter we will discuss:

- Integers and Division
- Primes
- Greatest Common Divisor
- Integers and Algorithms

Hello
World



- Of course, you already know what the integers are, and what division is...
- **But:** There are some specific notations, terminology, and theorems associated with these concepts which you may not know.
- These form the basics of *number theory*.
 - Vital in many important algorithms today (hash functions, cryptography, digital signatures).

Hello
World



Division

Hello
World



Division

- If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that $b = ac$.
 - When a divides b we say that
 - a is a **factor** of b and
 - b is a **multiple** of a .
 - The notation $a \mid b$ denotes that a divides b .
- **Examples:**
Let $x = 5$, $y = 10$, $z = 2$, $w = 15$, $v = 40$.
 - Does $x \mid y$? In other words, does $5 \mid 10$? **Yes!**
 - Does $x \mid w$? In other words, does $5 \mid 15$? **Yes!**
 - Does $z \mid x$? In other words, does $2 \mid 5$? **NO** – non-integer result

Hello
World



Division Theorem

Theorem : Let a , b , and c be integers.

Then

- if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
- if $a \mid b$, then $a \mid bc$ for all integers c ;
- if $a \mid b$ and $b \mid c$, then $a \mid c$.

Hello
World



Division Theorem

Theorem : Let a , b , and c be integers. Then

- if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;

- **Examples:**

Let $x = 5$, $y = 10$, $z = 2$, $w = 15$, $v = 40$.

- Does $x \mid y$? In other words, does $5 \mid 10$? **Yes!**
- Does $x \mid w$? In other words, does $5 \mid 15$? **Yes!**
- Since x divides both y and w , then x must also divide $(y + w)$.
In other words, 5 must divide $(10 + 15) = 25$, **which it does!**

- if $a \mid b$, then $a \mid bc$ for all integers c ;
- if $a \mid b$ and $b \mid c$, then $a \mid c$.

Hello
World



Division Theorem

Theorem : Let a , b , and c be integers. Then

- if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
- if $a \mid b$, then $a \mid bc$ for all integers c ;
 - **Examples:**
Let $x = 5$, $y = 10$, $z = 2$, $w = 15$, $v = 40$.
 - Does $x \mid y$? In other words, does $5 \mid 10$? **Yes!**
 - Since $x \mid y$, then x must divide yc , where c is any integer in \mathbb{Z} . Thus, x must divide yz or 5 must divide $10 \cdot 2 = 20$, **which it does!**
- if $a \mid b$ and $b \mid c$, then $a \mid c$.

Hello
World



Division Theorem

Theorem : Let a , b , and c be integers. Then

- if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
 - if $a \mid b$, then $a \mid bc$ for all integers c ;
 - if $a \mid b$ and $b \mid c$, then $a \mid c$.
- **Examples:**
 - Let $x = 5$, $y = 10$, $z = 2$, $w = 15$, $v = 40$.
 - Does $x \mid y$? In other words, does $5 \mid 10$? **Yes!**
 - Does $y \mid v$? In other words, does $10 \mid 40$? **Yes!**
 - Since $x \mid y$ and $y \mid v$, then x must divide v .
In other words, x must divide v or 5 must divide 40 ,
which it does!

Hello
World



Division Theorem

- **Corollary** : If a , b , and c be integers such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

- **Examples:**

Let $x = 5$, $y = 10$, $z = 2$, $w = 15$, $v = 40$.

- Since $x \mid y$ and $x \mid w$, then x must divide $my + nw$, for any integers, m and n .

In other words, if we choose $m = 3$ and $n=4$,
then x must divide $3y + 4w$

or 5 must divide $3*5 + 4*15 = 15 + 60 = 75$, **which it does!**

Hello
World



Primal Fear of Primes

Hello
World

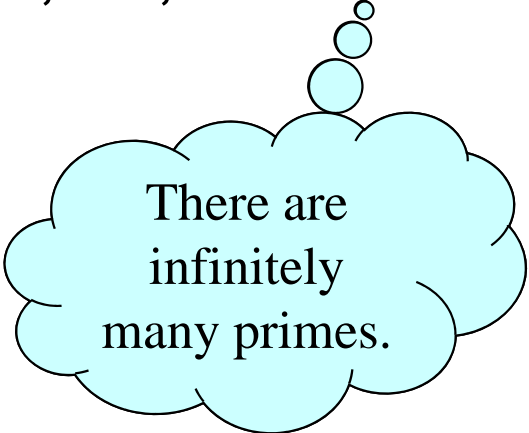


Primes

- = integer greater than 1 that is divisible only by 1 and itself.
- Examples:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29



**1 is NOT a
prime #!!!!**



There are
infinitely
many primes.

Hello
World



Primes

- A non-prime positive int greater than 1 is called **composite**.
- An integer n is composite if and only if there exists an integer a such that $a \mid n$ and $1 < a < n$
- Examples:
9 is composite because it is divisible by 3

**1 is NOT a
composite #
either!?!?!?**

If n is a composite integer, then n has a prime divisor less than or equal to \sqrt{n} .

Hello
World



Primes

- ***The Fundamental Theorem of Arithmetic:*** Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.
- Examples
 - $100 = 2 * 2 * 5 * 5 = 2^2 * 5^2$
 - $182 = 2 * 7 * 13$
 - $29820 = 2 * 2 * 3 * 5 * 7 * 71$
 - $641 = 641$
 - $999 = 3^3 * 37$
 - $1024 = 2^{10}$

What's up with this # 641?

PRIME!

Hello
World



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
 - None of these divide 113 evenly
 - Thus, by the fundamental theorem of arithmetic, 113 must be prime

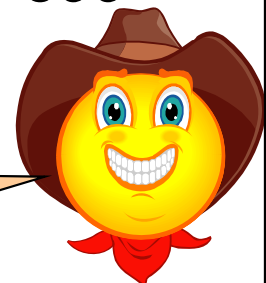
Hello
World



Showing a number is composite

- Show that 899 is prime
- Solution
 - Divide 899 by successively larger primes $< \sqrt{899}$, starting with 2
 - We find that 29 and 31 divide 899
- **FUN FACT:** On a unix system, enter “factor 899”
Prompt> factor 899
899: 29 31

What's the max number UNIX can factor?

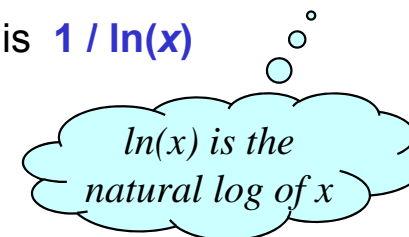


Hello
World



The prime number theorem

- The ratio 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
 - $\ln(10^{200}) \approx 460$
 - The chance of a 200 digit number being prime is $1/460$
 - If we only choose odd numbers, the chance is $2/460 = 1/230$



Hello
World



Greatest Common Divisors (*and* *Least Common Multiples*)

Hello
World



Division Algorithm

- The Division Algorithm Let a be an integer and d a positive integer.

Then there are unique integers q and r , with $0 \leq r < d$, such that $a = dq + r$.

- d is called the *divisor*,
- a is called the *dividend*,
- q is called the *quotient*,
- r is called the *remainder*.

- **Examples**

- $101 = 11 * 9 + 2.$
- $101 = 11 * 8 + 13?$
- $-11 = 3(-4) + 1.$
- $-11 = 3(-3) - 2?$

$$\begin{array}{r} Q \quad R \\ D \overline{) a} \end{array}$$

Hello
World



Division Algorithm

- **Examples:**

- Given $a = 13$ and $d = 4$,
what are the values of q and r ?
Since $13/4 = 3 + 1/4$, we know that

- $q = 13 \text{ div } 4 = 3$ and
- $r = 13 \text{ mod } 4 = 1$.

◦◦◦

*div is the same
as the integer /*

- Given $a = 96$ and $d = 15$,
what are the values of q and r ?
Since $97/15 = 6 + 7/15$, we know that

- $q = 97 \text{ div } 15 = 6$ and
- $r = 97 \text{ mod } 15 = 7$

◦◦◦


*mod is the same
as the integer %*

Hello
World



Greatest Common Denominator GCD

- The greatest common divisor of two integers a and b is the largest integer d such that $d \mid a$ and $d \mid b$
 - Denoted by $\text{gcd}(a,b)$
- Examples
 - $\text{gcd}(24, 36) = 12$
 - $\text{gcd}(17, 22) = 1$
 - $\text{gcd}(100, 17) = 1$



Easy way to
find gcd:
Find all positive
common
divisors of both
integers then
take the largest

Hello
World



Relatively Prime

- Two numbers are *relatively prime* if they don't have any common factors (other than 1)
 - Rephrased:
 a and b are relatively prime if $\text{gcd}(a,b) = 1$
- $\text{gcd}(25, 39) = 1$,
so 25 and 39 are relatively prime

Hello
World



Pairwise relative prime

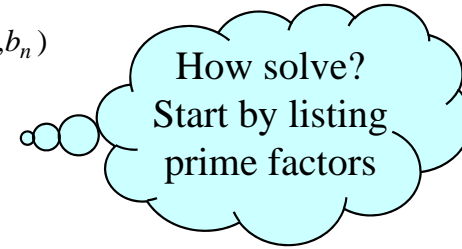
- A set of integers a_1, a_2, \dots, a_n are pairwise relatively prime if, for all pairs of numbers, they are relatively prime
 - Formally: The integers a_1, a_2, \dots, a_n are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.
- Example: are 10, 17, and 21 pairwise relatively prime?
 - $\gcd(10, 17) = 1$, $\gcd(17, 21) = 1$, and $\gcd(21, 10) = 1$
 - Thus, they are pairwise relatively prime
- Example: are 10, 19, and 24 pairwise relatively prime?
 - Since $\gcd(10, 24) \neq 1$, they are not

Hello
World



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 $\text{lcm}(a, b)$
 - $\text{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \dots p_n^{\max(a_n, b_n)}$
- Example: $\text{lcm}(10, 25) = 50$
- What is $\text{lcm}(95256, 432)$?
 - $95256 = 2^3 3^5 7^2$, $432 = 2^4 3^3$
 - $\text{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3, 4)} 3^{\max(5, 3)} 7^{\max(2, 0)} = 2^4 3^5 7^2 = 190512$



Hello
World



- Let a and b be positive integers.
Then $ab = \text{gcd}(a,b) * \text{lcm}(a,b)$

- Example:
 - $\text{gcd}(10,25) = 5,$
 $\text{lcm}(10,25) = 50$
 $10*25 = 5*50$

 - $\text{gcd}(95256, 432) = 216,$
 $\text{lcm}(95256, 432) = 190512$
 $95256*432 = 216*190512$

Hello
World



An Application of Primes!

- RSA Encryption

Hello
World



An Application of Primes!

- When you visit a secure web site (`https:...` address, indicated by padlock icon in IE, key icon in Netscape), the browser and web site may be using a technology called *RSA encryption*.
- This *public-key cryptography* scheme involves exchanging *public keys* containing the product pq of two random large primes p and q (a *private key*) which must be kept secret by a given party.
- So, the security of your day-to-day web transactions depends critically on the fact that all known factoring algorithms are intractable!
 - **Note:** There is a tractable *quantum* algorithm for factoring; so if we can ever build big quantum computers, then RSA is not secure.

Hello
World



Encrypting with public key

- I can generate public and private keys
- I publish my public key
- You can turn a message into a number and encrypt it
- Only I, who also know the private key, can decrypt it
- This solves one of the ancient problems of cryptography, going back to Greeks etc
 - how to first get the encryption “secret” from the recipient to the sender in a secure way

Hello
World



Simple application: secret emails

- Internet email is pretty insecure
- Anyone who can listen on the network can see what's in the emails as they go past
- But using public and private keys, people can encrypt a message and include it in an email
- Keys and messages are base64-encoded blobs of text like this:

```
-----BEGIN RSA PRIVATE KEY-----  
MIIBPAIBAAJBAOd5Zstqe+PGkfg4T8e3tDAr3ykv79ErTvERwFlO64/6IA5KkpMK  
FizFR3hZmnC8lrS+5DItdGkUo7y03mMMUsCAwEAAQJBAKQv0qA62cHJGcTtfHl3  
bpI0rEg0vnCpvYb1RnCSsDggo4Banb7/ak2a/QrvfWoyt4Y60PE/6ypGvgiy6eqM  
d+ECIQD8+88SCzXjDoNHxfjceTdeS2ZcA2xHdoL9179guWUM0wIhAOo78FEVh45/  
DagJRqXWNo81Sp1fk5LaIkmVXx2akh6pAiEAj2PCeH22K14cdt/1MDHceivOdrTR  
+KdPk6tno9Exp1UCIQChLwHeKjyP+CpDma596/y7a2afCOgaQ/UYQaukSXuHkQIq  
ZQFJimvH4ZZjErleQ+KsmyI2NuTk2/EDQxbnpyN35+g=  
-----END RSA PRIVATE KEY-----
```

Hello
World



Connecting with a key

- ssh uses RSA and similar algorithms
- Server generates a key pair to identify itself
- Users can generate key pairs to use instead of passwords
 - At CERN, SLAC etc, put your public key in `~/.ssh/authorized_keys`
- When you connect, ssh checks if server key pair is the same as last time
 - but, the first time, it has to take it on trust
 - would be better to use a signed certificate, rather than just a public key

Hello
World



Connecting with a certificate

- You're probably familiar with https websites
 - eg for credit card orders from Easyjet
- These use RSA etc to secure the connection
- Hosts have certificates rather than just public keys
 - in cert name have .../CN=www.easyjet.com
- So web browser can verify you're really giving your credit card number to Easyjet
- Also, if you put a user certificate into the browser, webserver can verify who you are

Hello
World



RSA: Guessing the Secret Key

Key Size (bits)	Number Of Keys	Time at 1 us each	Time at 1 ps each
32	4.3×10^9	35.8 min	2.15 ms
56	7.2×10^{16}	1142 yr	10 hr
128	3.4×10^{38}	5.4×10^{24} yr	5.4×10^{18} yr
168	3.7×10^{50}	5.9×10^{36} yr	5.9×10^{30} yr

Hello
World



The RSA Algorithm

- Select two primes **p** and **q**
- Calculate $n = p * q$
- Calculate $z = (p-1)(q-1)$
- Select **e** such that $1 < e < z$
and $\text{gcd}(z,e) = 1$ relatively prime
e has no common factors with z
- Calculate $d = e^{-1} \text{ mod } z$
- Public key $KU = \{e,n\}$
- Private key $KR = \{d,n\}$

*If $n=pq$ is very big,
I can't easily find
prime numbers
such that $p q = n$*

*Choose d such
that $ed-1$ is
exactly divisible
by z*

*if I don't know
 p and q , I
can't get d*

Hello
World



Example

compute e such that $ed = 1 \pmod{z}$,
 $\text{int-remdr}(ed) / ((p-1)(q-1)) = 1$,
i.e., $ed = k(p-1)(q-1) + 1$

- Select two primes $p=7$ and $q=17$
- Calculate $n = p * q$ $n = 119$
- Calculate $z = (p-1)(q-1)$ $z = 96$
- Select e such that $1 < e < z$
and $\text{gcd}(z,e) = 1$ $e = 5$
- Calculate $d = e^{-1} \pmod{z}$ $d = 77$
- Public key $KU = \{e,n\}$ $= \{5,119\}$
- Private key $KR = \{d,n\}$ $= \{77,119\}$

Hello
World



Example (continued)

$p=7$ and $q=17$

$n = 119$

$z = 96$

$e = 5$

$d = 77$

Public key $KU = \{e,n\} = \{5,119\}$

Private key $KR = \{d,n\} = \{77,119\}$

■ Plaintext $M = 19$

■ e was 5

■ To encrypt:

■ Ciphertext $C = M^e \bmod n = 19^5 \bmod 119 = 66$

■ To decrypt:

■ Plaintext $M = C^d \bmod n = 66^d \bmod 119$

$c = m^e \bmod n$
remainder when m
is divided by n

Hello
World



Cracking RSA

- Factor n , which is public, yielding p and q
- Calculate $z = (p-1)(q-1)$
- Calculate $d = e^{-1} \bmod z$ (e is public)
- Private key $KR = \{d, n\}$

Hello
World



Cracking RSA (Example)

- Factor 119, which is public, yielding 7 and 17
- Calculate $\phi(119) = (7-1)(17-1) = 96$
- Calculate $5^{-1} = 77 \pmod{96}$
- Private key $KR = \{77, 119\}$

Hello
World



Example (continued)

- Plaintext $M = 19$
- Ciphertext $C = M^e \bmod n = 19^5 \bmod 119 = 66$
- Plaintext $M = C^d \bmod n = 66^{77} \bmod 119 = 19$

Hello
World



So How Hard is Factoring?

Year	Decimal Digits	MIP-Years
1964	20	0.000009
1974	45	0.001
1984	71	0.1
1994	129	5000
?	2000	2.9×10^9

Hello
World



Modular Arithmetic

- If a and b are integers and m is a positive integer, then a is **congruent to b modulo m** if m divides $a-b$
 - Notation: $a \equiv b \pmod{m}$
 - Rephrased: $m \mid a-b$
 - Rephrased: $a \bmod m = b$
 - If they are not congruent: $a \not\equiv b \pmod{m}$
- Example: Is 17 congruent to 5 modulo 6?
 - Rephrased: $17 \equiv 5 \pmod{6}$
 - As 6 divides 17-5, they are congruent
- Example: Is 24 congruent to 14 modulo 6?
 - Rephrased: $24 \equiv 14 \pmod{6}$
 - As 6 does not divide $24-14 = 10$, they are not congruent

Hello
World



More on congruence

- Let a and b be integers, and let m be a positive integer.
Then $a \equiv b \pmod{m}$
if and only if $a \bmod m = b \bmod m$
 $a \% m = b \% m$
- Example:
Is 17 congruent to 5 modulo 6?
 - Rephrased: does $17 \equiv 5 \pmod{6}$?
 - $17 \bmod 6 = 5 \bmod 6$
- Example:
Is 24 congruent to 14 modulo 6?
 - Rephrased: $24 \equiv 14 \pmod{6}$
 - $24 \bmod 6 \neq 14 \bmod 6$

*The parenthesis
are required to
specify
modulus n .*

*'mod' and % are
the same*

**(mod m) is
NOT the
same as %**

Hello
World



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
 - You are substituting one letter with another

Hello
World



Algorithms

- 'algorithm' refers to a set of steps
- In programming, we use algorithms to define our programs
- An algorithm is also used to convert decimal numbers to binary or hexadecimal numbers and vice-versa.

- Since today's computers store values in binary, it helps if computer scientists can interpret binary values directly. Both octal and hexadecimal representations act as shortcuts toward this goal, by providing alternate methods for reading binary values.

Hello
World



Numerical Representations

- Since today's computers store values in binary, it helps if computer scientists can interpret binary values directly.
- Both octal and hexadecimal representations act as shortcuts toward this goal, by providing alternate methods for reading binary values.

Hello
World



Representation of Integers

- Let b be a positive integer greater than 1.
Then if n is a positive integer, it can be expressed uniquely in the form

$$n = a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b^1 + a_0$$

where k is a nonnegative integer,
 a_0, a_1, \dots, a_k are nonnegative integers less than b ,
and $a_k \neq 0$.

- Example – base 10
 - $496 = 4 * 10^2 + 9 * 10^1 + 6 * 10^0$

Hello
World



Binary Expansion

- A **binary expansion** of an integer happens when the integer b in the definition above has the value **2**.

Decimal Value	Binary Representation	Binary Value
0	$0 \cdot 2^0$	0_2
1	$1 \cdot 2^0$	1_2
2	$1 \cdot 2^1 + 0 \cdot 2^0$	10_2
3	$1 \cdot 2^1 + 1 \cdot 2^0$	11_2
4	$1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0$	100_2
5	$1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$	101_2
6	$1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$	110_2
7	$1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$	111_2
8	$1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0$	1000_2
9	$1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$	1001_2
10	$1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$	1010_2
11	$1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$	1011_2
12	$1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0$	1100_2
13	$1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$	1101_2
14	$1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$	1110_2
15	$1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$	1111_2
16	$1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0$	10000_2
17	$1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$	10001_2
18	$1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$	10010_2

Hello
World



Hex Expansion

- A **hexadecimal expansion** of an integer happens when the integer b in the definition above has the value 16 .

Decimal Value	Hexadecimal Representation	Hexadecimal Value
0	$0 \cdot 16^0$	0_{16}
1	$1 \cdot 16^0$	1_{16}
2	$2 \cdot 16^0$	2_{16}
3	$3 \cdot 16^0$	3_{16}
4	$4 \cdot 16^0$	4_{16}
5	$5 \cdot 16^0$	5_{16}
6	$6 \cdot 16^0$	6_{16}
7	$7 \cdot 16^0$	7_{16}
8	$8 \cdot 16^0$	8_{16}
9	$9 \cdot 16^0$	9_{16}
10	$10 \cdot 16^0$	A_{16}
11	$11 \cdot 16^0$	B_{16}
12	$12 \cdot 16^0$	C_{16}
13	$13 \cdot 16^0$	D_{16}
14	$14 \cdot 16^0$	E_{16}
15	$15 \cdot 16^0$	F_{16}
16	$1 \cdot 16^1 + 0 \cdot 16^0$	10_{16}
17	$1 \cdot 16^1 + 1 \cdot 16^0$	11_{16}
18	$1 \cdot 16^1 + 2 \cdot 16^0$	12_{16}

Hello
World



Practice

- Using integer division, provide **both** the quotient and the remainder when
 - 98 is divided by 10
 - 70 is divided by 22
- Are these integers prime?
 - 111
 - 113

Hello
World



Practice

- Provide the prime factorization for each of these integers:
 - 15
 - 97
 - 24

- Find the greatest common divisor for each pair of integers:
 - 15, 60
 - 32, 64

Hello
World



Practice

- Find the least common multiple for each pair of integers:
 - 3, 4
 - 30, 45
 - 3, 9, 21

- Convert these integers from decimal notation to binary notation:
 - 13
 - 67

Hello
World



Practice

- Convert these integers from binary notation to decimal notation:
 - 101100
 - 10001

Hello
World



Summary

- Division
- Prime
- Greatest Common Divisor
Least Common Multiple
- Congruence
- Caesar Cipher
- Binary Conversions
- Hexidecimal Conversions