SageMath 2: Number Theory

Cheng-Hsin Hsu

National Tsing Hua University

Department of Computer Science

Modular Arithmetic

- Example: $\underset{\textbf{Dividend}}{16} \div \underset{\textbf{Divisor}}{3} = \underset{\textbf{Quotient}}{5} \cdots \underset{\textbf{Remainder}}{1}$

- For any $a, b \in \mathbb{Z}, b > 0$, there exist unique $q, r \in \mathbb{Z}$ such that $a = qb + r,\ 0 \leqslant r < b$
- Modulo
  - $16 \mod 3 = 1$
  - $-12 \mod 5 = 3$

Modular Arithmetic in SageMath

```
25 // 4
```

6

Quotient

```
25 % 4
```

1

Modulo

```
4 * 6 + 1
```

25

Validation

Integers in Base Other than 10

- Write *6137* in the octal system (base *8*). In other words, finds $r_0, r_1, \ldots, r_k$ so that $(6137)_{10} = (r_k \ldots r_2 r_1 r_0)_8$
- Write *3387* into binary (base *2*) and hexadecimal (base *16*)

Divisor	Dividend	Remainders
8	6137	
8	767	$1(r_0)$
8	95	$7(r_1)$
8	11	$7(r_2)$
8	1	$3(r_3)$
	0	$1(r_4)$

Divisor	Dividend	Remainders	
16	13,874,945		
16	867,184	1	(r_0)
16	54,199	0	(r_1)
16	3,387	7	(r_2)
16	211	11 (= B)	(r_3)
16	13	3	(r_4)
	0	13 (= D)	(r_5)

Convert Integers into Other Bases

```
123.digits(base=16)
```

```
[11, 7]
```

```
123.digits(base=20)
```

```
[3, 6]
```

```
123.digits(base=60)
```

```
[3, 2]
```

```
3 + 2*60
```

```
123
```

Validation

Denominators for Exact Fractions

- Start from our familiar 10-based (decimal) system, for a fraction number *p/q* , we sometime can represent it exactly in two-decimal-place (or fewer)
  - 1/2 = 0.50
  - 1/3 = 0.33333333333333333333333333333333
  - 1/4 = 0.25
  - 1/5 = 0.20
- Any rules?? ← Hint: it has something to do with *q*

Divisors of 100

- Turns out that if $q \mid 100$, we can write p/q as a two-decimal-place exact decimal!
  - Why? Think about how you do division in tabular form!
- Let's use SageMath to find all divisors of 100

```
divisors(100)
```

```
[1, 2, 4, 5, 10, 20, 25, 50, 100]
```

- 9 out of 100? So, most of the time two decimals are not enough!

How About Other Bases

- Consider binary?

```
divisors(2^2)
```

- Base-20?

```
divisors(20^2)
```

```
[1, 2, 4, 5, 8, 10, 16, 20, 25, 40, 50, 80, 100, 200, 400]
```

- Base-60?

```
len(divisors(60^2))
```

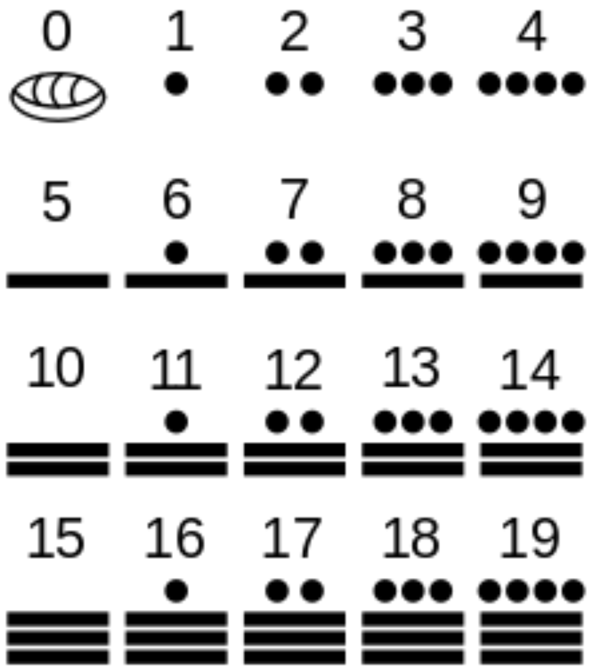
```
45
```

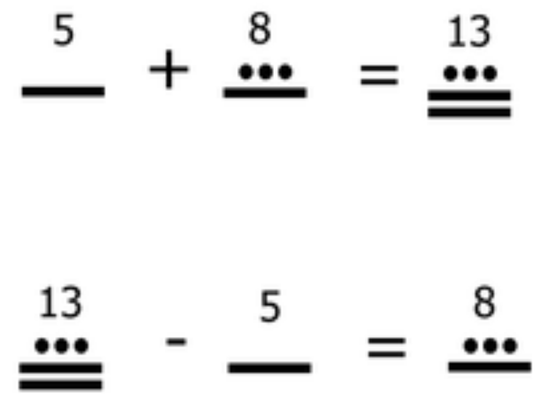
75%, better than 9%
In base-10 system!

$$\{1, 2, 3, 4, 5, 6, 8, 9, 10, 12, \ldots\}$$

- 60 is one of the highly composite numbers
  - Simplify counting, now 1/3 can be easily written!

Who Use Base-20 Systems?

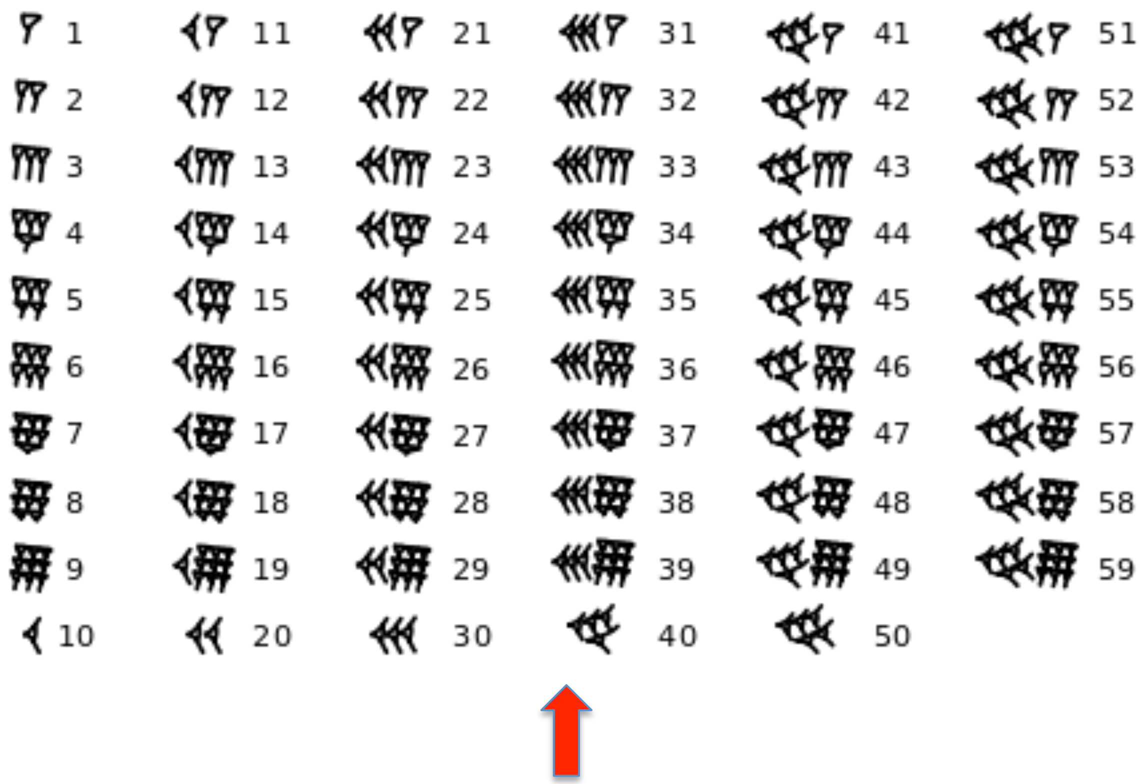




Maya Numerals

Source: https://en.wikipedia.org/wiki/Maya_numerals

How About Base-60 System?



Babylonian Numerals

- We still see base-60 systems in trigonometry and time metrics

Source: https://en.wikipedia.org/wiki/Babylonian_numerals

Prime and Composite

- Primes are integers (*n>1*) with exactly two positive divisors
- All other integers (*n>1*) are called composite
- If $n \in \mathbb{Z}^+$ is composite, then there is a prime *p* such that $p|n$

```
is_prime(123)
```

```
is_prime(179424673)
```

Prime Related Fun Functions

```
next_prime(123)
```

```
127
```

```
next_prime(10^100)
```

```
10000000000000000000000000000000000000000000000000000000000000000000000000\
00000000000000000000000000267
```

```
nth_prime(1)
```

evaluate

```
2
```

```
nth_prime(999)
```

```
7907
```

Prime Related Fun Functions (cont.)

```
prime_range(1,10)
```

```
[2, 3, 5, 7]
```

```
prime_range(1050, 1100)
```

```
[1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097]
```

```
factor(2015)
```

```
5 * 13 * 31
```

```
factor(-9999)
```

```
-1 * 3^2 * 11 * 101
```

Common Divisors

- For $a, b \in \mathbb{Z}$, $c > 0$ is a common divisor of *a* and *b* if $c|a \text{ and } c|b$
- Let $a, b \in \mathbb{Z}$, where $a \neq 0 \text{ or } b \neq 0$. Then $c \in \mathbb{Z}^+$ is a greatest common divisor (gcd) of *a* and *b* if
  - $c|a, c|b$
  - For any common divisor *d* of *a* and *b*, we know $d|c$
- For all $a, b \in \mathbb{Z}^+$, there exists a unique greatest common divisor of *a* and *b*, written as *gcd*(*a*,*b*)
  - it is actually the smallest positive integer that can is a linear combination of *a* and *b*

Common Multiples

- Let $a, b \in \mathbb{Z}^+$. *c* is a common multiple of a and *b*. *c* is the least common multiple if it is the smallest positive common multiple of *a*, b, we write *c*=*lcm*(*a,b*)

- If $a, b \in \mathbb{Z}^+$ and $c = \mathrm{lcm}(a, b)$. For any *d* that is a common multiple of *a* and *b*, we know

- For all $a, b \in \mathbb{Z}^+$, *ab*=lcm(*a,b*)gcd(*a,b*)

Fundamental Theorem of Arithmetic

- If $a, b \in \mathbb{Z}^+$ and *p* is a prime, then $p|ab \Rightarrow p|a \text{ or } p|b$
  - Can be generalized to *n* positive integers
- Any integer *n>1* can be written as a (unique) product of primes
  - Factorization
- Exercise: What is the prime factorization of 980220?
- Prove that *17|n* given

$$10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot n = 21 \cdot 20 \cdot 19 \cdot 18 \cdot 17 \cdot 16 \cdot 15 \cdot 14$$

Systematic Way to Find Gcd and Lcm

- Count the number of positive divisors of 360
  - Exercise: Find 2 ways to do this in SageMath, hint: *factor*(.) and *divisors*(.)
- Let $m = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}, n = p_1^{f_1} p_2^{f_2} \cdots p_t^{f_t}$, with $e_i, f_i \geqslant 0, \ \forall e_i, f_i$ we have

$$gcd(m,n) = \prod_{i=1}^{t} p_i^{a_i}, \text{ and } lcm(m,n) = \prod_{i=1}^{t} p_i^{b_i},$$

$$\text{where } a_i = \min(e_i, f_i), b_i = \max(e_i, f_i)$$

  - Find the gcd and lcm of $491891400 = 2^3 3^3 5^2 7^2 11^1 13^2$ and $1138845708 = 2^2 3^2 7^1 11^2 13^3 17^1$

SageMath Commands for Gcd and Lcm

```
gcd(120, 64)
```

8

```
lcm(120, 64)
```

960

```
gcd(gcd(120, 55), gcd(25, 35))
```

5

```
gcd([120, 55, 25, 35])
```

5

Relative Prime

- Integer *a* and *b* are relative prime if *gcd(a,b)=1*
  - If there exist integers *x* and *y*, so that *ax+by=1*

- Exercise: Check if 1234 and 8765 are relative prime in SageMath

```
gcd(1234,8765)
```

```
1
```

Euler's Phi Function

- We define $\phi(n)$ as the number of $1 \leq z \leq n$, where $\gcd(z, n) = 1$
  - What is $\phi(10)$?
- Write code to compute phi function

```
x = 10
cnt = 0
for n in xrange(1, x):
    if gcd(n, x) == 1:
        print n,
        cnt = cnt + 1
print
print 'phi(', x, ')=', cnt
```

```
1 3 7 9
phi( 10 )= 4
```

Euler's Phi Function (cont.)

- Try other x values for $\phi(x)$
- Suppose *x* and *y* are two distinct primes, what are the relation among $\phi(x), \phi(y), \text{ and } \phi(x \times y)$
- Actually, SageMath has a built-in phi function

```
euler_phi(10)
```

```
4
```

```
euler_phi(123)
```

```
80
```

Divisors of an Integer

- We define $\tau(x)$ be the number of divisors of *x*
- We define $\sigma(x)$ be the sum of all the divisors of *x*

```
divisors(250)
```

```
[1, 2, 5, 10, 25, 50, 125, 250]
```

```
len(divisors(250))
```

```
8
```

$\tau(250)$

```
sum(divisors(250))
```

$\sigma(250)$

```
468
```

Built-in Sigma Function

- Again, actually SageMath has a sigma function

```
divisors(45)
```

[1, 3, 5, 9, 15, 45]

```
sigma(45)
```

78

$$1 + 3 + 5 + 9 + 15 + 45 = 78$$

```
sigma(45, 2)
```

2366

$$1^2 + 3^2 + 5^2 + 9^2 + 15^2 + 45^2 = 2366$$

```
sigma(45, 0)
```

6

What is this?

$$1^0 + 3^0 + 5^0 + 9^0 + 15^0 + 45^0 = 6$$

Congruence

- If *a* and *b* have the same remainder upon division by *n*, *a* is *congruent* to *b* modulo *n*
  - Written as $a \equiv b \pmod{n}$
  - That is $n|(a-b)$

- Example
  - $23 \equiv 8 \pmod{5}$
  - $5|(23-8)$

Amicable Pairs of Numbers

- An interesting Arab tradition: put two numbers 220 and 284 on their rings and give them to their spouses

$$\text{divisors}(\boxed{220}) = \{1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110, 220\}$$

$$1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = \boxed{284}$$

$$\text{divisors}(\boxed{284}) = \{1, 2, 4, 71, 142, 284\}$$

$$1 + 2 + 4 + 71 + 142 = \boxed{220}$$

Summary

- We introduced various number theory functions in SageMath
- We will use them to introduce some cryptography results
- References:
  - http://www.sagemath.org ← Official Web and resources
  - http://www.gregorybard.com/SAGE.html ← Our textbook

SageMath #2 Homework (S2)

1. (2%) Write a SageMath program to find out at least 3 amicable pairs, including (220, 284)
2. (1%) Euclidean algorithm is a well-known algorithm calculating gcd of two integers. Implement it in SageMath and solve gcd(312500, 12768). Your program has to print individual steps. Hint: one version of the pseudocode looks like this:

```
function gcd(a, b)
    while b ≠ 0
        t := b
        b := a mod b
        a := t
    return a
```