Elementary Number Theory

- **Modulo Arithmetic (definition, properties, & different notation)**

Elementary Number Theory

- **Modulo Arithmetic (definition, properties, & different notation)**
- **Computing $a^m \pmod{n}$**

Elementary Number Theory

- **Modulo Arithmetic (definition, properties, & different notation)**
- **Computing $a^m \pmod{n}$**
- **Euler's Phi Function (definition, formula)**

Theorem (G. Martin). *The smallest positive integer n that satisfies $\phi(30n+1) < \phi(30n)$ is*

n=232,909,810,175,496,793,814,049,684,205,233,780,004,859,885,966,051,235,363,345,311,
075,888,344,528,723,154,527,984,260,176,895,854,182,634,802,907,109,271,610,432,287,
652,976,907,467,574,362,400,134,090,318,355,962,121,476,785,712,891,544,538,210,966,
704,036,990,885,292,446,155,135,679,717,565,808,063,766,383,846,220,120,606,143,826,
509,433,540,250,085,111,624,970,464,541,380,934,486,375,688,208,918,750,640,674,629,
942,465,499,369,036,578,640,331,759,035,979,369,302,685,371,156,272,245,466,396,227,
865,621,951,101,808,240,692,259,960,203,091,330,589,296,656,888,011,791,011,416,062,
631,565,320,593,772,287,118,913,728,608,997,901,791,216,356,108,665,476,306,080,740,
121,528,236,888,680,120,152,479,138,327,451,088,404,280,929,048,314,912,122,784,879,
758,304,016,832,436,751,532,255,185,640,249,324,065,492,491,511,072,521,585,980,547,

```
> evalf((1-1/2)*(1-1/3)*(1-1/5))
.2666666667
> ithprime(4)
7
> evalf(product((1-1/ithprime(j)),j=4..384))
.2667113307
```

Elementary Number Theory

- **Modulo Arithmetic (definition, properties, & different notation)**
- **Computing $a^m \pmod{n}$**
- **Euler's Phi Function (definition, formula)**
- **Euler's Theorem, Fermat's Little Theorem, and the Existence of Inverses**

Elementary Number Theory

- **Modulo Arithmetic (definition, properties, & different notation)**
- **Computing $a^m \pmod{n}$**
- **Euler's Phi Function (definition, formula)**
- **Euler's Theorem, Fermat's Little Theorem, and the Existence of Inverses**
- **Computing Inverses (later)**
- **Chinese Remainder Theorem**

Elementary Number Theory

- **Modulo Arithmetic (definition, properties, & different notation)**
- **Computing $a^m \pmod{n}$**
- **Euler's Phi Function (definition, formula)**
- **Euler's Theorem, Fermat's Little Theorem, and the Existence of Inverses**
- **Computing Inverses (later)**
- **Chinese Remainder Theorem**
- **Generators exist modulo 2, 4, p^e, and $2p^e$**

Algorithm from Knuth, Vol. 2, p. 320

Algorithm A ***(Modern Euclidean algorithm).*** **Given nonnegative integers u and v, this algorithm finds their greatest common divisor.**

A1. [Check v = 0] If $v = 0$, the algorithm terminates with u as the answer.

A2. [Take u mod v] Set $r \leftarrow u \bmod v$, $u \leftarrow v$, $v \leftarrow r$, and return to A1. (The operations of this step decrease the value of v, but they leave $\gcd(u, v)$ unchanged.)

Theorem (Lamé). ***Let $\phi = (1 + \sqrt{5})/2$. Let $0 \leq u, v < N$ in Algorithm A. Then the number of times step A2 is repeated is $\leq \lfloor \log_\phi(\sqrt{5}N) \rfloor - 2$.***