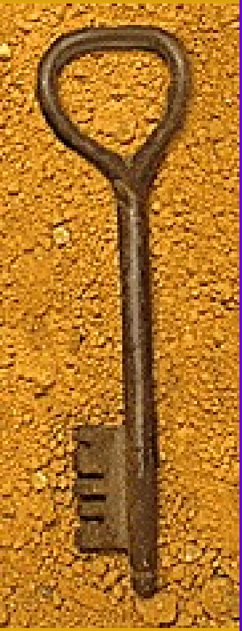
Fermat and Euler’s Theorems

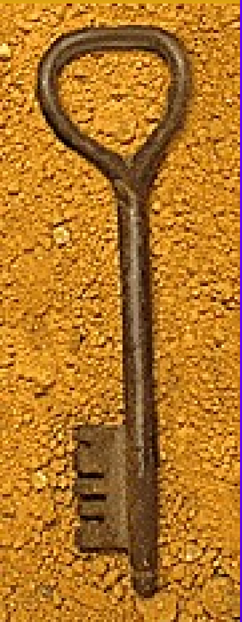


Prime Numbers

- A prime number is divisible only by 1 and itself
- For example: {2, 3, 5, 7, 11, 13, 17, …}
- 1 could also be considered prime, but it’s not very useful.

Prime Factorization

- To factor a number *n* is to write it as a product of other numbers.
- $n = a * b * c$
- Or, 100 = 5 * 5 * 2 * 2
- Prime factorization of a number *n* is writing it as a product of prime numbers.
- 143 = 11 * 13



Relatively Prime Numbers

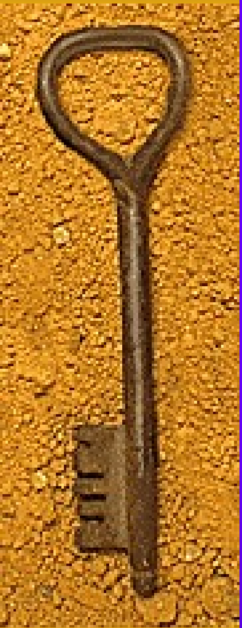
- Two numbers are relatively prime if they have no common divisors other than 1.
- 10 and 21 are relatively prime, in respect to each other, as 10 has factors of 1, 2, 5, 10 and 21 has factors of 1, 3, 7, 21.
- The Greatest Common Divisor (GCD) of two relatively prime numbers can be determined by comparing their prime factorizations and selecting the least powers.

Relatively Prime Numbers Cont.

- For example, $125 = 5^3$ and $200 = 2^3 * 5^2$
- $GCD(125, 200) = 2^0 * 5^2 = 25$
- If the two numbers are relatively prime the GCD will be 1.
- Consider the following: 10(1, 2, 5, 10) and 21(1, 3, 7, 21)
- $GCD(10, 21) = 1$
- It then follows, that a prime number is also relatively prime to any other number other than itself and 1.

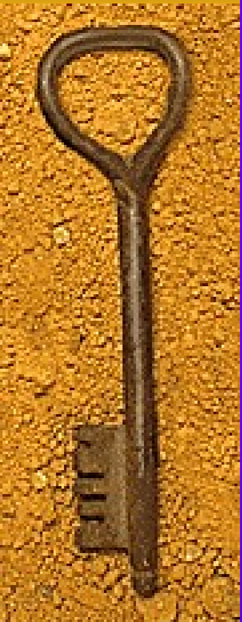
Fermat’s Little Theorem

- If p is prime and a is an integer not divisible by p, then . . .
- $a^{p-1} \equiv 1 \pmod{p}$.
- And for every integer a
- $a^{p} \equiv a \pmod{p}$.
- This theorem is useful in public key (RSA) and primality testing.



Euler Totient Function: $\phi(n)$

- $\phi(n)$ = how many numbers there are between 1 and n-1 that are relatively prime to n.
- $\phi(4) = 2$ (1, 3 are relatively prime to 4)
- $\phi(5) = 4$ (1, 2, 3, 4 are relatively prime to 5)
- $\phi(6) = 2$ (1, 5 are relatively prime to 6)
- $\phi(7) = 6$ (1, 2, 3, 4, 5, 6 are relatively prime to 7)

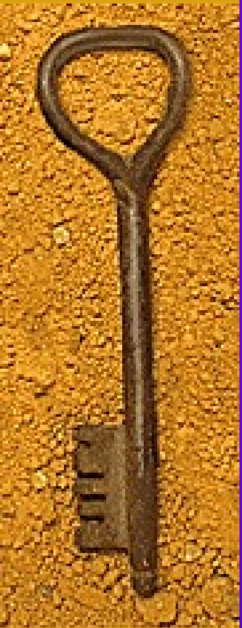


Euler Totient Function Cont.

- As you can see from $\phi(5)$ and $\phi(7)$, $\phi(n)$ will be n-1 whenever n is a prime number. This implies that $\phi(n)$ will be easy to calculate when n has exactly two different prime factors: $\phi(P * Q) = (P-1)*(Q-1)$, if P and Q are prime.

Euler’s Totient Theorem

- This theorem generalizes Fermat’s theorem and is an important key to the RSA algorithm.
- If GCD(a, p) = 1, and $a < p$, then $a^{\phi(p)} \equiv 1 (\text{mod } p)$.
- In other words, If a and p are relatively prime, with a being the smaller integer, then when we multiply a with itself $\phi(p)$ times and divide the result by p, the remainder will be 1.



Euler’s Totient Theorem Cont.

- Let’s test the theorem:
- If $a = 5$ and $p = 6$
- Then $\phi(6) = (2-1) * (3-1) = 2$
- So, $5^{\phi(6)} = 25$ and $25 = 24+1 = 6*4+1$
- => 25 = 1(mod 6) OR 25 % 6 = 1
- It also follows that $a^{\phi(p)+1} \equiv a(\text{mod } p)$ so that p does not necessarily need to be relatively prime to a.