Primes

- Positive integers that have exactly two different positive integer factors (1 and itself) are called **primes**.
- An integer p greater than 1 is called ***prime*** if the only positive factors of p are 1 and p.
- A positive integer that is greater than 1 and is not prime is called ***composite***.
- Ex. Prime No. 3, 5, 7, 11 etc.

Trial Division

One procedure for showing that an integer is prime is based on the following observation.

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

Ex. Show that 101 is prime.

The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, and 7. Because 101 is not divisible by 2, 3, 5, or 7.

THE FUNDAMENTAL THEOREM OF ARITHMETIC

Every 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.

Ex. The prime factorizations of 100, 641, 999, and 1024 are -

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2252$

$641 = 641$

$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 33 \cdot 37$

$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

Ex. Find the prime factorization of 7007.

Greatest Common Divisors and Least Common Multiples

The largest integer that divides both of two integers is called the **greatest common divisor** of these integers.

Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

Ex.1 What is the greatest common divisor of 24 and 36?

Solution: The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6, and 12. Hence, $\gcd(24, 36) = 12$.

Ex.2 What is the greatest common divisor of 17 and 22?

Solution: The integers 17 and 22 have no positive common divisors other than 1, so that $\gcd(17, 22) = 1$.

The Euclidean Algorithm

The algorithm is based on below facts.

- If we subtract smaller number from larger (we reduce larger number), GCD doesn't change. So if we keep subtracting repeatedly the larger of two, we end up with GCD.
- Now instead of subtraction, if we divide with smaller number, the algorithm stops when we find remainder 0.

```
int gcd(int a, int b)
{
      if (a == 0)
            return b;
      return gcd(b % a, a);
}
```

Let $a = bq + r$, where a, b, q, and r are integers.
Then gcd$(a, b) =$ gcd(b, r).

ALGORITHM 1 The Euclidean Algorithm

procedure *gcd*(*a, b*: positive integers)
$x := a$
$y := b$
while $y \mathrel{!}= 0$
      $r := x$ **mod** y
      $x := y$
      $y := r$
return x {gcd(a, b) is x}

Ex. Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

Ans:

$a = b \cdot q + r$

$662 = 414 \cdot 1 + 248$

$414 = 248 \cdot 1 + 166$

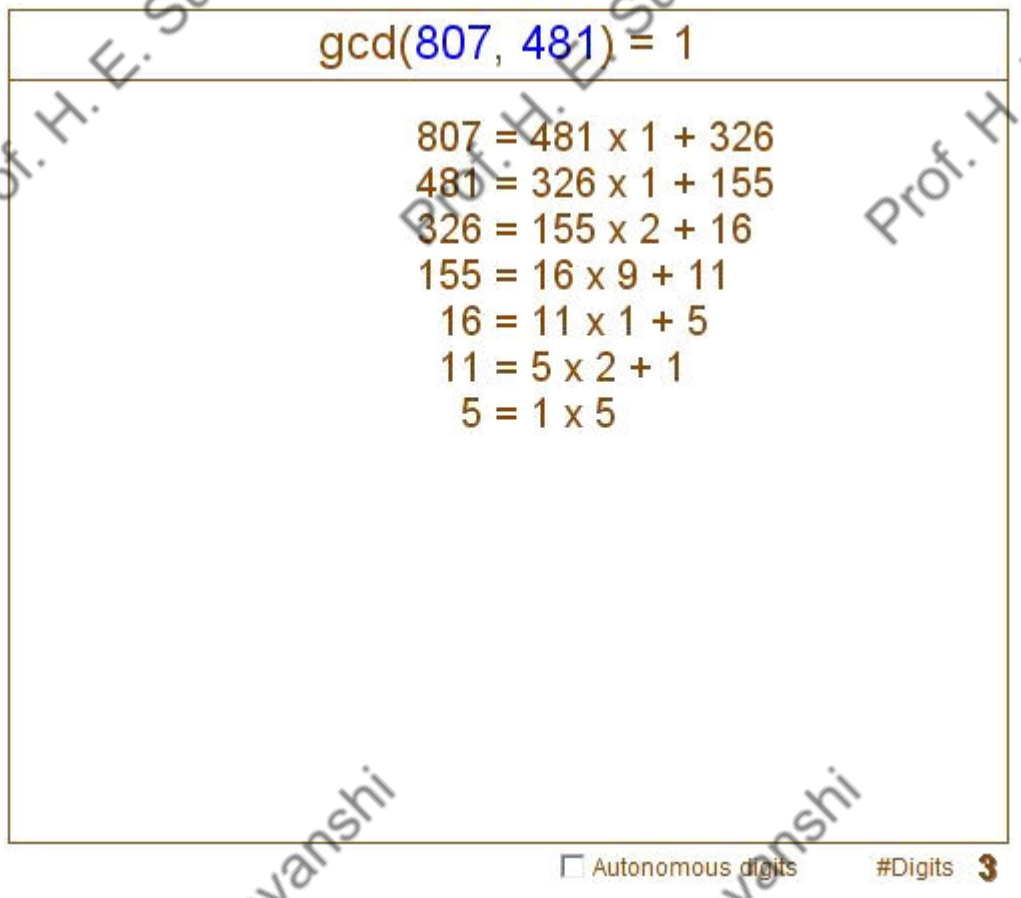
$248 = 166 \cdot 1 + 82$

$166 = 82 \cdot 2 + 2$

$82 = 2 \cdot 41 + 0$

Hence, gcd(414, 662) = 2, because 2 is the last nonzero remainder.

The integers *a* and *b* are *relatively prime* if their greatest common divisor is 1



Problems

1. Determine whether each of these integers is prime.
a) 21 **b)** 29 **c)** 71 **d)** 97 **e)** 111 **f)** 143

2. Determine whether each of these integers is prime.
a) 19 **b)** 27 **c)** 93 **d)** 101 **e)** 107 **f)** 113

3. Find the prime factorization of each of these integers.
a) 88 **b)** 126 **c)** 729 **d)** 1001 **e)** 1111

4. Find the prime factorization of each of these integers.
a) 39 **b)** 81 **c)** 101 **d)** 143 **e)** 289 **f)** 899

5. Determine whether the integers in each of these sets are pairwise relatively prime.
a) 21, 34, 55 **b)** 14, 17, 85
c) 25, 41, 49, 64 **d)** 17, 18, 19, 23

6. Determine whether the integers in each of these sets are pairwise relatively prime.
a) 11, 15, 19 **b)** 14, 15, 21
c) 12, 17, 31, 37 **d)** 7, 8, 9, 11