Number Theory

Definition. *A **prime number** is a positive integer $p > 1$ whose only divisors are 1 and itself. A **composite number** is a positive integer with some positive divisor other than 1 and itself. The number 1 is neither prime nor composite.*

As of January 2020, the largest known prime number is $2^{82,589,933} - 1$, a number with $24,862,048$ digits. In contrast, the number of elementary particles in the universe is a number with approximately 80 digits only.

The density of the primes decreases the further along the number line we travel. Do the primes eventually cease? No, by a celebrated result of Euclid.

Theorem. *There are infinitely many primes.*

Definition. *We call the largest divisor of a set of integers their **greatest common divisor** or **highest common factor**. When the greatest common divisor of a set of integers is 1, we refer to those integers as **relatively prime** or **coprime**.*

Definition. *We call the smallest positive multiple of a set of integers their **least common multiple**.*

Theorem (Fundamental Theorem of Arithmetic). *Any integer $n > 1$ may be written as*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

for e_i some positive integers and p_i some distinct primes. The decomposition is unique up to ordering.

Theorem. *Let $m, n \in \mathbb{N}$ and suppose their prime factorizations are given by*

$$m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$
$$n = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$$

(some e_i, f_i might be zero here). Then we have the following formulas

$$\gcd(m,n) = p_1^{\min\{e_1,f_1\}} p_2^{\min\{e_2,f_2\}} \cdots p_k^{\min\{e_k,f_k\}},$$
$$\operatorname{lcm}(m,n) = p_1^{\max\{e_1,f_1\}} p_2^{\max\{e_2,f_2\}} \cdots p_k^{\max\{e_k,f_k\}}.$$

Theorem (Divisibility Tests). *Let $n \in \mathbb{N}$*

(i) n is divisible by 1 always.
(ii) n is divisible by 2 if and only if its last digit is 0,2,4,6 or 8.
(iii) n is divisible by 3 if and only if the sum of its digits is divisible by 3.
(iv) n is divisible by 4 if and only if the number formed by its last two digits is divisible by 4.
(v) n is divisible by 5 if and only if its last digit is 0 or 5.
(vi) n is divisible by 6 if and only if it is divisible by both 2 and 3.
(vii) n is divisible by 7 if and only if subtracting twice the last digit from the number formed by the remaining digits produces a number which is divisible by 7.
(viii) n is divisible by 8 if and only if the number formed by its last three digits is divisible by 8.
(ix) n is divisible by 9 if and only if the sum of its digits is divisible by 9.
(x) n is divisible by 10 if and only if its last digit is 0.
(xi) n is divisible by 11 if and only if the alternating sum of its digits is divisible by 11.

Theorem. *Suppose $n \in \mathbb{N}$ has the prime decomposition*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

Then n is a perfect square if and only if $e_1, e_2, \ldots e_k$ are all divisible by 2. Similarly, n is a perfect cube if and only if $e_1, e_2, \ldots e_k$ are all divisible by 3.

Theorem. *Suppose $n \in \mathbb{N}$ has the prime decomposition*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

Then the number of factors of n is given by

$$(e_1 + 1)(e_2 + 2) \cdots (e_k + 1).$$

Theorem (Division Algorithm). *For any $n, d \in \mathbb{N}$ there exists unique $q, r \in \mathbb{N} \cup \{0\}$ with $0 \leq r < d$ such that*

$$n = qd + r.$$

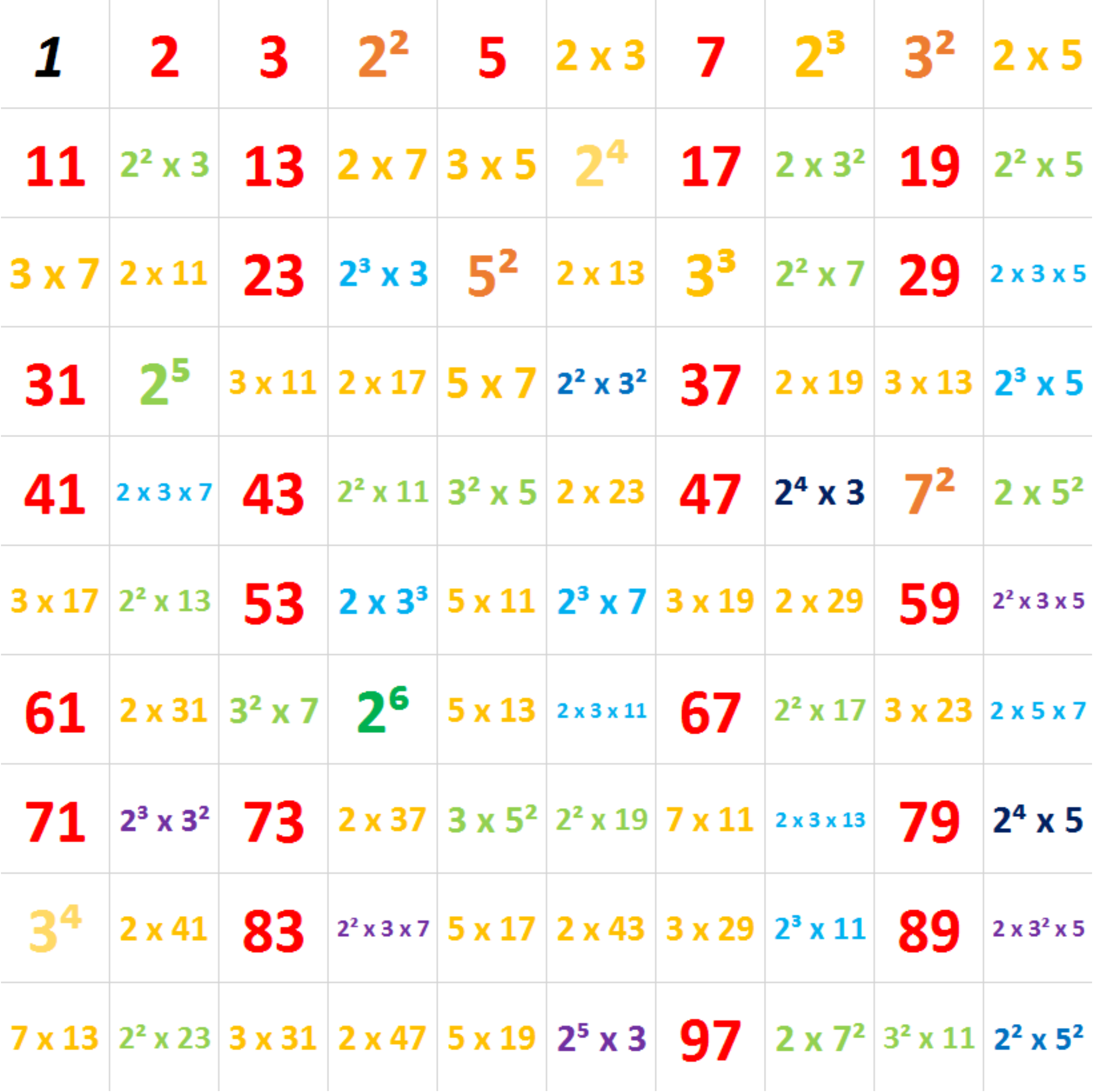
THEOREM. *Suppose $a, b \in \mathbb{N}$. If $b = aq + r$, where $r, q \in \mathbb{N} \cup \{0\}$, then*

$$\gcd(a, b) = \gcd(a, b - a) = \cdots = \gcd(a, r).$$

This states that the gcd of two numbers is invariant if the large number is replaced by its difference with the smaller number. In particular, this gives an efficient procedure for determining the gcd of two integers known as the **Euclidean Algorithm**. This is best illustrated via an example. Suppose we seek to determine $\gcd(18, 25)$. Then, thanks to the above theorem, the following computations show that this must be equal to 1.

$$\begin{aligned} 25 &= 1 \times 18 + 7 \\ 18 &= 2 \times 7 + 4 \\ 7 &= 1 \times 4 + 3 \\ 4 &= 1 \times 3 + 1 \\ 3 &= 3 \times 1 \end{aligned}$$

The diagram below shows the prime factorizations for positive integers up to 100.



1	2	3	2^2	5	2 x 3	7	2^3	3^2	2 x 5
11	2^2 x 3	13	2 x 7	3 x 5	2^4	17	2 x 3^2	19	2^2 x 5
3 x 7	2 x 11	23	2^3 x 3	5^2	2 x 13	3^3	2^2 x 7	29	2 x 3 x 5
31	2^5	3 x 11	2 x 17	5 x 7	2^2 x 3^2	37	2 x 19	3 x 13	2^3 x 5
41	2 x 3 x 7	43	2^2 x 11	3^2 x 5	2 x 23	47	2^4 x 3	7^2	2 x 5^2
3 x 17	2^2 x 13	53	2 x 3^3	5 x 11	2^3 x 7	3 x 19	2 x 29	59	2^2 x 3 x 5
61	2 x 31	3^2 x 7	2^6	5 x 13	2 x 3 x 11	67	2^2 x 17	3 x 23	2 x 5 x 7
71	2^3 x 3^2	73	2 x 37	3 x 5^2	2^2 x 19	7 x 11	2 x 3 x 13	79	2^4 x 5
3^4	2 x 41	83	2^2 x 3 x 7	5 x 17	2 x 43	3 x 29	2^3 x 11	89	2 x 3^2 x 5
7 x 13	2^2 x 23	3 x 31	2 x 47	5 x 19	2^5 x 3	97	2 x 7^2	3^2 x 11	2^2 x 5^2

Image Attribution: `https://thechalkfaceblog.files.wordpress.com/2015/03/primesonlycolour.png`