ACHS Math Team

Notes on Factoring and Prime Numbers

Peter S. Simon

1 November 2007

Prime Numbers—The Sieve of Eratosthenes

Recall that the prime numbers are natural numbers having exactly two distinct factors (the number itself and 1). The most efficient way to find all of the small primes (say all those less than 10,000,000) is by using the Sieve of Eratosthenes (ca 240 BC):

1. Start with a list of natural numbers from 2 to, say, 37.
   2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37

Prime Numbers—The Sieve of Eratosthenes

Recall that the prime numbers are natural numbers having exactly two distinct factors (the number itself and 1). The most efficient way to find all of the small primes (say all those less than 10,000,000) is by using the Sieve of Eratosthenes (ca 240 BC):

1. Start with a list of natural numbers from 2 to, say, 37.
   2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37
2. The first number 2 is prime. Retain it, but cross out all multiples of 2 in the list.
   $\boxed{2}$ 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~ 19 ~~20~~ 21 ~~22~~ 23 ~~24~~ 25 ~~26~~ 27 ~~28~~ 29 ~~30~~ 31 ~~32~~ 33 ~~34~~ 35 ~~36~~ 37

Prime Numbers—The Sieve of Eratosthenes

Recall that the prime numbers are natural numbers having exactly two distinct factors (the number itself and 1). The most efficient way to find all of the small primes (say all those less than 10,000,000) is by using the Sieve of Eratosthenes (ca 240 BC):

1. Start with a list of natural numbers from 2 to, say, 37.
   2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37
2. The first number 2 is prime. Retain it, but cross out all multiples of 2 in the list.
   $\boxed{2}$ 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~ 19 ~~20~~ 21 ~~22~~ 23 ~~24~~ 25 ~~26~~ 27 ~~28~~ 29 ~~30~~ 31 ~~32~~ 33 ~~34~~ 35 ~~36~~ 37
3. The first remaining number 3 is prime. Retain it, but cross out all multiples of 3 in the list.
   $\boxed{2}$ $\boxed{3}$ ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ 25 ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~ 31 ~~32~~ ~~33~~ ~~34~~ 35 ~~36~~ 37

Prime Numbers—The Sieve of Eratosthenes (Cont.)

4. The first remaining number 5 is prime. Retain it, but cross out all multiples of 5 in the list.
   $\boxed{2}$ $\boxed{3}$ $\cancel{4}$ $\boxed{5}$ $\cancel{6}$ 7 $\cancel{8}$ $\cancel{9}$ $\cancel{10}$ 11 $\cancel{12}$ 13 $\cancel{14}$ $\cancel{15}$ $\cancel{16}$ 17 $\cancel{18}$ 19 $\cancel{20}$ $\cancel{21}$ $\cancel{22}$ 23 $\cancel{24}$ $\cancel{25}$ $\cancel{26}$ $\cancel{27}$ $\cancel{28}$ 29 $\cancel{30}$ 31 $\cancel{32}$ $\cancel{33}$ $\cancel{34}$ $\cancel{35}$ $\cancel{36}$ 37

Prime Numbers—The Sieve of Eratosthenes (Cont.)

4. The first remaining number 5 is prime. Retain it, but cross out all multiples of 5 in the list.
   $\boxed{2}$ $\boxed{3}$ $\cancel{4}$ $\boxed{5}$ $\cancel{6}$ 7 $\cancel{8}$ $\cancel{9}$ $\cancel{10}$ 11 $\cancel{12}$ 13 $\cancel{14}$ $\cancel{15}$ $\cancel{16}$ 17 $\cancel{18}$ 19 $\cancel{20}$ $\cancel{21}$ $\cancel{22}$ 23 $\cancel{24}$ $\cancel{25}$ $\cancel{26}$ $\cancel{27}$ $\cancel{28}$ 29 $\cancel{30}$ 31 $\cancel{32}$ $\cancel{33}$ $\cancel{34}$ $\cancel{35}$ $\cancel{36}$ 37
5. The first remaining number 7 is prime. Retain it, but cross out all multiples of 7 in the list.
   $\boxed{2}$ $\boxed{3}$ $\cancel{4}$ $\boxed{5}$ $\cancel{6}$ $\cancel{7}$ $\cancel{8}$ $\cancel{9}$ $\cancel{10}$ 11 $\cancel{12}$ 13 $\cancel{14}$ $\cancel{15}$ $\cancel{16}$ 17 $\cancel{18}$ 19 $\cancel{20}$ $\cancel{21}$ $\cancel{22}$ 23 $\cancel{24}$ $\cancel{25}$ $\cancel{26}$ $\cancel{27}$ $\cancel{28}$ 29 $\cancel{30}$ 31 $\cancel{32}$ $\cancel{33}$ $\cancel{34}$ $\cancel{35}$ $\cancel{36}$ 37

Prime Numbers—The Sieve of Eratosthenes (Cont.)

4. The first remaining number 5 is prime. Retain it, but cross out all multiples of 5 in the list.
   $\boxed{2}\ \boxed{3}\ \cancel{4}\ \boxed{5}\ \cancel{6}\ 7\ \cancel{8}\ \cancel{9}\ \cancel{10}\ 11\ \cancel{12}\ 13\ \cancel{14}\ \cancel{15}\ \cancel{16}\ 17\ \cancel{18}\ 19\ \cancel{20}\ \cancel{21}\ \cancel{22}\ 23\ \cancel{24}\ \cancel{25}\ \cancel{26}\ \cancel{27}\ \cancel{28}\ 29\ \cancel{30}\ 31\ \cancel{32}\ \cancel{33}\ \cancel{34}\ \cancel{35}\ \cancel{36}\ 37$
5. The first remaining number 7 is prime. Retain it, but cross out all multiples of 7 in the list.
   $\boxed{2}\ \boxed{3}\ \cancel{4}\ \boxed{5}\ \cancel{6}\ \cancel{7}\ \cancel{8}\ \cancel{9}\ \cancel{10}\ 11\ \cancel{12}\ 13\ \cancel{14}\ \cancel{15}\ \cancel{16}\ 17\ \cancel{18}\ 19\ \cancel{20}\ \cancel{21}\ \cancel{22}\ 23\ \cancel{24}\ \cancel{25}\ \cancel{26}\ \cancel{27}\ \cancel{28}\ 29\ \cancel{30}\ 31\ \cancel{32}\ \cancel{33}\ \cancel{34}\ \cancel{35}\ \cancel{36}\ 37$
6. The first remaining number is $11 > \sqrt{37}$ so we do not need to check for multiples of it or any of the other remaining numbers in the list (why?). All the remaining numbers in the list are primes:
   $2, 3, 5, 7, 11, 13, 17, 23, 29, 31, 37$

GCF: Greatest Common Factor

The greatest common factor (GCF) of two natural numbers is the greatest factor that divides both of the numbers.

Examples: $\mathrm{GCF}(2,3) = 1, \quad \mathrm{GCF}(2,4) = 2, \quad \mathrm{GCF}(10,15) = 5.$

GCF: Greatest Common Factor

The greatest common factor (GCF) of two natural numbers is the greatest factor that divides both of the numbers.

Examples: $\text{GCF}(2,3) = 1, \quad \text{GCF}(2,4) = 2, \quad \text{GCF}(10,15) = 5.$

To find the GCF of two numbers:

GCF: Greatest Common Factor

The greatest common factor (GCF) of two natural numbers is the greatest factor that divides both of the numbers.

Examples: $\text{GCF}(2, 3) = 1, \quad \text{GCF}(2, 4) = 2, \quad \text{GCF}(10, 15) = 5.$

To find the GCF of two numbers:

1. List the prime factors of each number. Include all prime factors in both lists (may require a zero exponent).

GCF: Greatest Common Factor

The greatest common factor (GCF) of two natural numbers is the greatest factor that divides both of the numbers.

Examples: $\mathrm{GCF}(2,3) = 1, \quad \mathrm{GCF}(2,4) = 2, \quad \mathrm{GCF}(10,15) = 5.$

To find the GCF of two numbers:

1. List the prime factors of each number. Include all prime factors in both lists (may require a zero exponent).
2. Multiply each factor the lesser number of times that it occurs in either factor.

GCF: Greatest Common Factor

The greatest common factor (GCF) of two natural numbers is the greatest factor that divides both of the numbers.

Examples: $\text{GCF}(2,3) = 1, \quad \text{GCF}(2,4) = 2, \quad \text{GCF}(10,15) = 5.$

To find the GCF of two numbers:

1. List the prime factors of each number. Include all prime factors in both lists (may require a zero exponent).
2. Multiply each factor the lesser number of times that it occurs in either factor.

- Example: Find $\text{GCF}(90,24)$

GCF: Greatest Common Factor

The greatest common factor (GCF) of two natural numbers is the greatest factor that divides both of the numbers.

Examples: $\mathrm{GCF}(2,3) = 1$, $\mathrm{GCF}(2,4) = 2$, $\mathrm{GCF}(10,15) = 5$.

To find the GCF of two numbers:

1. List the prime factors of each number. Include all prime factors in both lists (may require a zero exponent).
2. Multiply each factor the lesser number of times that it occurs in either factor.

- Example: Find $\mathrm{GCF}(90,24)$
- Prime factors of 90: $2^1 \times 3^2 \times 5^1$

GCF: Greatest Common Factor

The greatest common factor (GCF) of two natural numbers is the greatest factor that divides both of the numbers.

Examples: $GCF(2,3) = 1, \quad GCF(2,4) = 2, \quad GCF(10,15) = 5.$

To find the GCF of two numbers:

1. List the prime factors of each number. Include all prime factors in both lists (may require a zero exponent).
2. Multiply each factor the lesser number of times that it occurs in either factor.

- Example: Find $GCF(90,24)$
- Prime factors of 90: $2^1 \times 3^2 \times 5^1$
- Prime factors of 24: $2^3 \times 3^1 \times 5^0$

GCF: Greatest Common Factor

The greatest common factor (GCF) of two natural numbers is the greatest factor that divides both of the numbers.

Examples: $\mathrm{GCF}(2,3) = 1, \quad \mathrm{GCF}(2,4) = 2, \quad \mathrm{GCF}(10,15) = 5.$

To find the GCF of two numbers:

1. List the prime factors of each number. Include all prime factors in both lists (may require a zero exponent).
2. Multiply each factor the lesser number of times that it occurs in either factor.

- Example: Find $\mathrm{GCF}(90,24)$
- Prime factors of 90: $2^1 \times 3^2 \times 5^1$
- Prime factors of 24: $2^3 \times 3^1 \times 5^0$
- Therefore, $\mathrm{GCF}(90,24) = 2^1 \times 3^1 \times 5^0 = 6.$

LCM: Least Common Multiple

A common multiple is a number that is a multiple of two or more numbers. The common multiples of 3 and 4 are $0, 12, 24, \ldots$ The least common multiple (LCM) of two numbers is the smallest number (not zero) that is a multiple of both. So $\text{LCM}(3, 4) = 12$.

To find the LCM of two numbers:

1. List the prime factors of each number. Include all prime factors in both lists (may reqire a zero exponent).

LCM: Least Common Multiple

A common multiple is a number that is a multiple of two or more numbers. The common multiples of 3 and 4 are $0, 12, 24, \ldots$ The least common multiple (LCM) of two numbers is the smallest number (not zero) that is a multiple of both. So $\text{LCM}(3, 4) = 12$.

To find the LCM of two numbers:

1. List the prime factors of each number. Include all prime factors in both lists (may reqire a zero exponent).
2. Multiply each factor the greater number of times that it occurs in either factor.

LCM: Least Common Multiple

A common multiple is a number that is a multiple of two or more numbers. The common multiples of 3 and 4 are $0, 12, 24, \ldots$ The least common multiple (LCM) of two numbers is the smallest number (not zero) that is a multiple of both. So $\text{LCM}(3, 4) = 12$.

To find the LCM of two numbers:

1. List the prime factors of each number. Include all prime factors in both lists (may reqire a zero exponent).
2. Multiply each factor the greater number of times that it occurs in either factor.

- Example: Find $\text{LCM}(90, 24)$

LCM: Least Common Multiple

A common multiple is a number that is a multiple of two or more numbers. The common multiples of 3 and 4 are $0, 12, 24, \ldots$ The least common multiple (LCM) of two numbers is the smallest number (not zero) that is a multiple of both. So $\text{LCM}(3, 4) = 12$.

To find the LCM of two numbers:

1. List the prime factors of each number. Include all prime factors in both lists (may reqire a zero exponent).
2. Multiply each factor the greater number of times that it occurs in either factor.

- Example: Find $\text{LCM}(90, 24)$
- Prime factors of 90: $2^1 \times 3^2 \times 5^1$

LCM: Least Common Multiple

A common multiple is a number that is a multiple of two or more numbers. The common multiples of 3 and 4 are $0, 12, 24, \ldots$ The least common multiple (LCM) of two numbers is the smallest number (not zero) that is a multiple of both. So $\text{LCM}(3, 4) = 12$.

To find the LCM of two numbers:

1. List the prime factors of each number. Include all prime factors in both lists (may reqire a zero exponent).
2. Multiply each factor the greater number of times that it occurs in either factor.

- Example: Find $\text{LCM}(90, 24)$
- Prime factors of 90: $2^1 \times 3^2 \times 5^1$
- Prime factors of 24: $2^3 \times 3^1 \times 5^0$

LCM: Least Common Multiple

A common multiple is a number that is a multiple of two or more numbers. The common multiples of 3 and 4 are $0, 12, 24, \ldots$ The least common multiple (LCM) of two numbers is the smallest number (not zero) that is a multiple of both. So $\text{LCM}(3, 4) = 12$.

To find the LCM of two numbers:

1. List the prime factors of each number. Include all prime factors in both lists (may reqire a zero exponent).
2. Multiply each factor the greater number of times that it occurs in either factor.

- Example: Find $\text{LCM}(90, 24)$
- Prime factors of 90: $2^1 \times 3^2 \times 5^1$
- Prime factors of 24: $2^3 \times 3^1 \times 5^0$
- Therefore, $\text{LCM}(90, 24) = 2^3 \times 3^2 \times 5^1 = 360.$

Product of GCF and LCM

Note that

$$\mathrm{GCF}(90, 24) \times \mathrm{LCM}(90, 24) = 6 \times 360 = 2160 = 90 \times 24$$

This is true in general:

$$\boxed{\mathrm{GCF}(a, b) \times \mathrm{LCM}(a, b) = a \times b}$$

The product of the GCF and LCM of two natural numbers is equal to the product of the numbers themselves.

Proof that GCF$(M, N) \times$ LCM$(M, N) = MN$

Let M and N be positive integers, and let $\{P_1, P_2, \ldots, P_k\}$ be the set of all prime factors of either M or N. Then M and N can be factored as

Proof that GCF$(M, N) \times$ LCM$(M, N) = MN$

Let M and N be positive integers, and let $\{P_1, P_2, \ldots, P_k\}$ be the set of all prime factors of either M or N. Then M and N can be factored as

$$M = P_1^{m_1} \times P_2^{m_2} \times \cdots \times P_k^{m_k}$$
$$N = P_1^{n_1} \times P_2^{n_2} \times \cdots \times P_k^{n_k}$$

Proof that GCF$(M, N) \times$ LCM$(M, N) = MN$

Let M and N be positive integers, and let $\{P_1, P_2, \ldots, P_k\}$ be the set of all prime factors of either M or N. Then M and N can be factored as

$$M = P_1^{m_1} \times P_2^{m_2} \times \cdots \times P_k^{m_k}$$
$$N = P_1^{n_1} \times P_2^{n_2} \times \cdots \times P_k^{n_k}$$

The GCF and LCM are

$$\mathrm{GCF}(M, N) = P_1^{\min(m_1, n_1)} \times P_2^{\min(m_2, n_2)} \times \cdots \times P_k^{\min(m_k, n_k)}$$
$$\mathrm{LCM}(M, N) = P_1^{\max(m_1, n_1)} \times P_2^{\max(m_2, n_2)} \times \cdots \times P_k^{\max(m_k, n_k)}$$

Proof that GCF$(M, N) \times$ LCM$(M, N) = MN$

Let M and N be positive integers, and let $\{P_1, P_2, \ldots, P_k\}$ be the set of all prime factors of either M or N. Then M and N can be factored as

$$M = P_1^{m_1} \times P_2^{m_2} \times \cdots \times P_k^{m_k}$$
$$N = P_1^{n_1} \times P_2^{n_2} \times \cdots \times P_k^{n_k}$$

The GCF and LCM are

$$\mathrm{GCF}(M, N) = P_1^{\min(m_1, n_1)} \times P_2^{\min(m_2, n_2)} \times \cdots \times P_k^{\min(m_k, n_k)}$$
$$\mathrm{LCM}(M, N) = P_1^{\max(m_1, n_1)} \times P_2^{\max(m_2, n_2)} \times \cdots \times P_k^{\max(m_k, n_k)}$$

Since for any pair of integers m and n, $\min(m, n) + \max(m, n) = m + n$, then

Proof that GCF$(M, N) \times$ LCM$(M, N) = MN$

Let M and N be positive integers, and let $\{P_1, P_2, \ldots, P_k\}$ be the set of all prime factors of either M or N. Then M and N can be factored as

$$M = P_1^{m_1} \times P_2^{m_2} \times \cdots \times P_k^{m_k}$$
$$N = P_1^{n_1} \times P_2^{n_2} \times \cdots \times P_k^{n_k}$$

The GCF and LCM are

$$\mathrm{GCF}(M, N) = P_1^{\min(m_1, n_1)} \times P_2^{\min(m_2, n_2)} \times \cdots \times P_k^{\min(m_k, n_k)}$$
$$\mathrm{LCM}(M, N) = P_1^{\max(m_1, n_1)} \times P_2^{\max(m_2, n_2)} \times \cdots \times P_k^{\max(m_k, n_k)}$$

Since for any pair of integers m and n, $\min(m, n) + \max(m, n) = m + n$, then

$$\begin{aligned} \mathrm{GCF}(M, N)\,\mathrm{LCM}(M, N) &= P_1^{m_1+n_1} \times P_2^{m_2+n_2} \times \cdots \times P_k^{m_k+n_k} \\ &= MN \end{aligned}$$

Finding the Prime Decomposition of an Integer

For large integers this is a very hard problem. In fact, the difficulty of this problem is at the heart of several important cryptographic systems. For example, the record for factoring a 200-digit number is held by a team at the German Federal Agency for Information Technology Security. It took them several months on a supercomputer to factor this *semiprime* (a product of two primes) number. Larger semiprime numbers are beyond the capability of the foreseeable state of the art.

Finding the Prime Decomposition of an Integer

For large integers this is a very hard problem. In fact, the difficulty of this problem is at the heart of several important cryptographic systems. For example, the record for factoring a 200-digit number is held by a team at the German Federal Agency for Information Technology Security. It took them several months on a supercomputer to factor this *semiprime* (a product of two primes) number. Larger semiprime numbers are beyond the capability of the foreseeable state of the art.

For a smaller integer n, such as those you are likely to encounter in math competitions, *trial division* is a simple algorithm. Simply try dividing the integer by all prime numbers less than or equal to $\sqrt{n}$. Of course, this technique is faster when you have memorized the first few primes, say, those under 100.