Prime Factorizations and Divisibility

Ryan C. Daileda

Trinity University

Number Theory

Introduction

The Fundamental Theorem of Arithmetic (FTA) completely describes the multiplicative structure of $\mathbb{N}$.

By relaxing the uniqueness requirement of the FTA somewhat, we can the connect (modified) canonical forms of integers to divisibility theory.

This will yield (modified) canonical expressions for the GCD and LCM, and related them to each other.

Canonical Forms and Divisibility

Recall that the *canonical form* of a natural number $a \geq 2$ is

$$a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

in which each p_i is distinct and $a_i \in \mathbb{N}$ for all i.

The FTA guarantees that canonical forms exist and are unique.

It can be convenient to allow $a_i \in \mathbb{N}_0$, although this changes the statement of the FTA somewhat.

For instance 60 has the *modified canonical* forms

$$60 = 2^2 \cdot 3 \cdot 5 = 2^2 \cdot 3 \cdot 5 \cdot 7^0 = 2^2 \cdot 3 \cdot 5 \cdot 13^0 \cdot 19^0.$$

Now even 1 has prime factorizations:

$$1 = 2^0 = 3^0 = 5^0 \cdot 7^0 \cdot 13^0.$$

Theorem 1 (FTA for Modified Canonical Forms)

Every $n \in \mathbb{N}$ can be expressed in the form

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

where the p_i are distinct primes and $a_i \in \mathbb{N}_0$. The primes and exponents for which $a_i > 0$ are unique.

The advantage of modified canonical forms is that they allow us to express any given (finite) set of natural numbers using the same collection of primes.

As an application of this idea, let $a \in \mathbb{N}$ and suppose $d \in \mathbb{N}$ divides a.

If a prime p divides d, then it divides a as well, by transitivity of divisibility.

Therefore the primes occurring in the "true" canonical form of d must be among those of a.

So if we write

$$a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

with distinct p_i and $a_i \geq 0$, we can also write

$$d = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r},$$

but with $d_i \geq 0$.

Write $a = de$ with $e \in \mathbb{N}$. Since $e|a$ as well, similar remarks apply to e:

$$e = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

with $e_i \geq 0$.

We therefore have

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = a = de = p_1^{d_1+e_1} p_2^{d_2+e_2} \cdots p_r^{d_r+e_r}.$$

If $a_i > 0$ or $d_i + e_i > 0$, then uniqueness in the modified FTA imply that $a_i = d_i + e_i$. Otherwise $a_i = d_i + e_i = 0$.

So, in any case, $a_i = d_i + e_i$. Since $a_i, d_i, e_i \in \mathbb{N}_0$, this implies that

$$a_i \geq d_i \quad \text{for all } i.$$

Conversely, if $a_i \geq d_i$ for all i, then $a_i - d_i \in \mathbb{N}_0$ so that

$$e = p_1^{a_1-d_1} p_2^{a_2-d_2} \cdots p_r^{a_r-d_r} \in \mathbb{N},$$

and

$$de = p_1^{d_1+(a_1-d_1)} p_2^{d_2(a_2-d_2)} \cdots p_r^{d_r+(a_r-d_r)} = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = a.$$

That is, we have constructed a divisor of a from the exponents d_i.

Theorem 2

If $a \in \mathbb{N}$ has the modified canonical form $a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, then $d \in \mathbb{N}$ divides a if and only if $d = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r}$ with $0 \leq d_i \leq a_i$ for all i.

We now have a complete description of the set of (positive) divisors of a in terms of its canonical form.

Example 1

Determine all the divisors of 2600.

Solution. A little work gives the canonical form

$$2600 = 2^3 \cdot 5^2 \cdot 13.$$

So the divisors of 2600 have the form

$$2^a \cdot 5^b \cdot 13^c,$$

where $0 \leq a \leq 3$, $0 \leq b \leq 2$ and $0 \leq c \leq 1$.

So we have $4 \cdot 3 \cdot 2 = 24$ divisors:

1	2	$2^2 = 4$
$2^3 = 8$	5	$2 \cdot 5 = 10$
$2^2 \cdot 5 = 20$	$2^3 \cdot 5 = 40$	$5^2 = 25$
$2 \cdot 5^2 = 50$	$2^2 \cdot 5^2 = 100$	$2^3 \cdot 5^2 = 200$
13	$2 \cdot 13 = 26$	$2^2 \cdot 13 = 52$
$2^3 \cdot 13 = 104$	$5 \cdot 13 = 65$	$2 \cdot 5 \cdot 13 = 130$
$2^2 \cdot 5 \cdot 13 = 260$	$2^3 \cdot 5 \cdot 13 = 520$	$5^2 \cdot 13 = 325$
$2 \cdot 5^2 \cdot 13 = 650$	$2^2 \cdot 5^2 \cdot 13 = 1300$	$2^3 \cdot 5^2 \cdot 13 = 2600$

Remarks

Taking the notion of modified canonical form to its extreme, we find that we can write any $a \in \mathbb{N}$ uniquely in the form

$$a = \prod_p p^{a_p},$$

where the product runs over all the prime numbers, $a_p \in \mathbb{N}_0$ for all p, and *only finitely many* $a_p \neq 0$.

The map $a \mapsto (a_p)_p$ carrying each natural number to its sequence of exponents yields a bijection

$$E : \mathbb{N} \to \sum_p \mathbb{N}_0$$

of $\mathbb{N}$ with the *direct sum* of a countable number of copies of $\mathbb{N}_0$.

Because multiplication of natural numbers adds the exponents in their modified canonical forms, we find that E is, in fact, an isomorphism (multiplicative to additive) of *monoids*:

$$E(1) = (0, 0, 0, \ldots),$$
$$E(ab) = (a_p + b_p)_p = (a_p)_p + (b_p)_p = E(a) + E(b).$$

So the *multiplicative* structure of $\mathbb{N}$ is identical to the *additive* structure of $\sum_p \mathbb{N}_0$.

For instance, the partial order $a|b$ on $\mathbb{N}$ immediately translates to a partial order on $\sum_p \mathbb{N}_0$:

$$(a_p)_p \preceq (b_p)_p \quad \Leftrightarrow \quad a_p \leq b_p \text{ for all primes } p.$$

Counting Divisors

Theorem 2 has the following immediate consequence.

Corollary 1

Let $a \in \mathbb{N}$ and write it in modified canonical form $a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. Then a has exactly

$$(a_1 + 1)(a_2 + 1) \cdots (a_r + 1)$$

positive divisors.

Remark. Note that the inclusion of extraneous primes in the modified canonical form doesn't change the value of the product, since $0 + 1 = 1$.

Proof. Theorem 2 tells us that the divisors of a are given by

$$d = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r},$$

with $0 \leq d_i \leq a_i$ for all i.

Since there are $a_i + 1$ choices for d_i, for each i, the result follows. □

Example 2

How many positive divisors does 1484325 have?

Solution. Since $1484325 = 3^4 \cdot 5^2 \cdot 733$, there are exactly $5 \cdot 3 \cdot 2 = 30$ positive divisors. □

Canonical Forms and GCDs

Let $a, b \in \mathbb{N}$ and write their modified canonical forms as

$$a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$
$$b = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}.$$

According to Theorem 2, $d \in \mathbb{N}$ is a common divisor of a and b if and only if $d = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r}$ with

$$0 \leq d_i \leq a_i \quad \text{and} \quad 0 \leq d_i \leq b_i \quad \Leftrightarrow \quad 0 \leq d_i \leq \min\{a_i, b_i\}.$$

for all i. It follows at once that

$$\boxed{(a, b) = p_1^{\min\{a_1, b_1\}} p_2^{\min\{a_2, b_2\}} \cdots p_r^{\min\{a_r, b_r\}}}$$

Remark. This result is primarily of theoretical importance. To actually compute the GCD it is much more efficient to use the EA.

Example 3

Use canonical forms to compute $(7181350, 1292870)$.

Solution. We have

$$7181350 = 2 \cdot 5^2 \cdot 11^2 \cdot 1187 = 2^1 \cdot 5^2 \cdot 11^2 \cdot 1187^1 \cdot 129287^0,$$
$$1292870 = 2 \cdot 5 \cdot 129287 = 2^1 \cdot 5^1 \cdot 11^0 \cdot 1187^0 \cdot 129287^1.$$

Thus

$$(7181350, 1292870) = 2^1 \cdot 5^1 \cdot 11^0 \cdot 1187^0 \cdot 129287^0 = 10.$$

□

Least Common Multiples

Dual to the notion of greatest common divisor is the least common multiple.

Let $a, b \in \mathbb{N}$. We define their *least common multiple* (LCM) to be the smallest $m \in \mathbb{N}$ so that

$$a|m \quad \text{and} \quad b|m.$$

We denote the LCM of a and b by $[a, b]$.

Because $a|ab$ and $b|ab$, the $[a, b]$ exists by the Well-Ordering Principle.

We can express the LCM in terms of canonical forms, and will use this to connect it to the GCD.

Write a, b and $[a, b]$ in modified canonical form:

$$\begin{aligned} a &= p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}, \\ b &= p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}, \\ [a, b] &= p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}. \end{aligned}$$

Since $a|[a, b]$ and $b|[a, b]$, Theorem 2 tells us that

$$a_i \leq c_i \quad \text{and} \quad b_i \leq c_i \quad \Leftrightarrow \quad c_i \geq \max\{a_i, b_i\}$$

for all i. So, to make $[a, b]$ as small as possible, it must be that

$$c_i = \max\{a_i, b_i\}$$

for all i.

That is,

$$\boxed{[a, b] = p_1^{\max\{a_1, b_1\}} p_2^{\max\{a_2, b_2\}} \cdots p_r^{\max\{a_r, b_r\}}.}$$

As with the GCD, this isn't the best way to find the LCM. It's better to go through the GCD via the EA.

Notice that for all i we have

$$a_i + b_i = \max\{a_i, b_i\} + \min\{a_i, b_i\}.$$

It immediately follows that

$$\boxed{ab = (a, b)[a, b].}$$

Example 4

Compute $[9780, 9234]$.

Solution. It takes 7 divisions in the EA to find that

$$(9780, 9234) = 6.$$

Thus

$$[9780, 9234] = \frac{9780 \cdot 9234}{(9780, 9234)} = \frac{90308520}{6} = \boxed{15051420.}$$