A little more about divisibility

One need not use unique factorization into primes to prove things like the following important and often-used fact.

**Proposition:** If \( \gcd(d, a) = 1 \) and \( d|ab \) then \( d|b \).

**Proof:** This proof is very similar to the proof that if \( p \) is prime and does not divide \( a \) but \( p|ab \) then \( p|b \).

Let \( r, s \) be integers such that \( rd + sa = 1 \), from the peculiar characterization of \( \gcd \).
Let \( ab = Nd \). Then

\[
b = b \cdot 1 = b \cdot (rd + sa)
\]

\[
= drb + sab = drb + sNd = d(rb + Ns)
\]

so \( d \) divides \( b \). ///
Equality modulo \( m \)

To understand the interaction of reduction modulo \( m \) with addition and multiplication:

*Gauss was the first to notice that divisibility properties can be recast as a kind of equality, thereby making use of our prior experience with manipulation of equalities.*

Recall that \( x \% m \) is an operation which accepts ordinary integer inputs and produces an integer output.

**Equality modulo \( m \) is a relation**

\[
x = y \mod m \quad \text{if and only if} \quad m | (x - y)
\]

Sometimes this is written with *three* lines instead of two, as in

\[
x \equiv y \mod m
\]

and called a congruence. But it is really a modified form of equality. Think of \( \mod m \) as an *adverb* modifying the verb *equals.*
For example,

\[
\begin{align*}
2 & \equiv 7 \mod 5 \quad \text{because } 5|(2 - 7) \\
12 & \equiv 7 \mod 5 \quad \text{because } 5|(12 - 7) \\
127 & \equiv 7 \mod 5 \quad \text{because } 5|(127 - 7) \\
-123 & \equiv 127 \mod 5 \quad \text{because } 5|(-123 - 127)
\end{align*}
\]

Although the definition does not explicitly compare equality modulo \( m \) with reduction modulo \( m \), there is a simple connection:

**Lemma:** \( x \equiv y \mod m \) if and only if \( x \% m = y \% m \).

**Proof:** If \( m|(x - y) \) and if \( x = qm + r \) and \( y = q'm + r' \) with \( 0 \leq r < |m| \) and \( 0 \leq r' < |m| \), then \( m|(qm + r - q'm - r') \) and \( m|(r - r') \). Since \( r \) and \( r' \) are non-negative and smaller than \( m \), it must be that \( r = r' \). Thus \( x \% m = y \% m \). On the other hand, if \( x \% m = y \% m \) then \( m|(r - r') \) and \( m|(qm + r - q'm - r') \), so \( m|x - y \). 

///
Equivalence relations, equivalence classes

For fixed modulus \( m \), \( x = y \mod m \) is an **equivalence relation** in the sense that

\[
    x = x \mod m \quad \text{(Reflexivity)}
\]

\[
    x = y \mod m \text{ implies } y = x \mod m \quad \text{(Symmetry)}
\]

\[
    x = y \mod m \text{ and } y = z \mod m \text{ implies } x = z \mod m \quad \text{(Transitivity)}
\]

The **equivalence class** of congruence class or **residue class** of \( x \) modulo \( m \) is the set of all integers \( x' \) equal to \( x \) modulo \( m \). It is often denoted \( \bar{x} \) without explicit reference to the modulus. And \( x \mod m \) may refer to this set. Thus,

\[
    x \mod m = \bar{x} = \{ x' \in \mathbb{Z} : x' = x \mod m \}
\]

\[
    = \{ \ldots, x - 2m, x - m, x, x + m, x + 2m, \ldots \}
\]

*There is no explicit reference to reduction modulo \( m \) in this.*
For example,

\[ 2 \text{ mod } 5 = \{\ldots, -8, -3, 2, 7, 12, \ldots\} \]
\[ -1 \text{ mod } 5 = \{\ldots, -6, -1, 4, 9, 14, \ldots\} \]
\[ 4 \text{ mod } 5 = \{\ldots, -6, -1, 4, 9, 14, \ldots\} \]
\[ 9 \text{ mod } 5 = \{\ldots, -6, -1, 4, 9, 14, \ldots\} \]
\[ 5 \text{ mod } 5 = \{\ldots, -10, -5, 0, 5, 10, \ldots\} \]
\[ 0 \text{ mod } 5 = \{\ldots, -10, -5, 0, 5, 10, \ldots\} \]

But the mental picture of one of these \textit{equivalence classes} should be as a \textit{single entity}, not an infinite set.
Well-definedness of arithmetic mod $m$

To prove that reduction modulo $m$ interacts well with addition and multiplication, we really prove, instead, that addition and multiplication (and subtraction) are well-defined modulo $m$.

Well-definedness is not a concept that one meets in more elementary mathematics, but it comes up often in modern mathematics. The point is that something that appears to be a reasonable definition as output of an operation may fail by secretly specifying more than one output. One way that this frequently occurs is in a situation where objects have many different names, by specifying the output in terms of one name, but getting different outputs depending on which name of the same object is used.

We want the outcome to depend on the object, not on a name for it.
In the case at hand, we want to prove that

If \( x = x' \mod m \) and \( y = y' \mod m \), then
- \( x + y = x' + y' \mod m \)
- \( x \cdot y = x' \cdot y' \mod m \)

In other words, we claim that if \( x, y, x', y' \) are integers with \( \overline{x} = \overline{x'} \) and \( \overline{y} = \overline{y'} \) then
- \( \overline{x + y} = \overline{x' + y'} \)
- \( \overline{x \cdot y} = \overline{x' \cdot y'} \)

That is, the equivalence class of a sum or product does not depend on the name we use for equivalence classes, but only upon the equivalence classes themselves.

Thus, we have an addition and multiplication of equivalence classes modulo \( m \).
This well-definedness implies that reduction modulo $m$ interacts well with addition and multiplication. To show that

\[(x \% m) + (y \% m)) \% m = (x + y) \% m\]

note that $z \% m = z \mod m$ for any $z \in \mathbb{Z}$. With $z = (x \% m) + (y \% m)$ gives

\[
((x \% m) + (y \% m)) \% m = (x \% m) + (y \% m) \mod m
\]

With $z = x \% m$ and $z = y \% m$, using well-definedness of addition modulo $m$, this becomes

\[= x + y \mod m\]

Similarly, using the principle with $z = x + y$, the right-hand side is

\[(x + y) \% m = x + y \mod m\]

Thus, the two things are equal modulo $m$, which by an earlier observation implies that their reductions modulo $m$ are the same.
Algebra modulo $m$

Equality modulo $m$ has advantages in computations.

For example, let’s compute the ones’-place digit of $3^{616}$. First, realize that the ones’-place digit of an integer $n$ is nothing other than $n \% 10$. So we want $3^{616} \% 10$.

Note that we have no reason to think that the 616 in the exponent can be reduced modulo 10.

Note that if you attempt to have your calculator/computer compute $3^{616}$ first, and look at the ones’-place digit, even if you don’t get an overflow error the roundoff error will lead you to believe that the ones’-place digit is 0. That is, you might think that 10 divides a large power of 3. How likely is this, given unique factorization into primes? Ha.
To evaluate $3^{616} \% 10$ we should experiment a little with powers of 3 modulo 10:

$$3^2 = 9 \mod 10$$
$$3^3 = 7 \mod 10$$
$$3^4 = 1 \mod 10$$

The fact that $3^4 = 1 \mod 10$ allows us to do the following:

$$3^{616} = 3^{4 \cdot 154} = (3^4)^{154}$$

$$= 1^{154} \mod 10 = 1 \mod 10$$

So the ones’-place digit of $3^{616}$ is 1.

Similarly, the ones’-place digit of $3^{714}$ can be computed as

$$3^{714} = 3^{4 \cdot 178+2} = (3^4)^{178} \cdot 3^2$$

$$= 1^{178} \cdot 3^2 \mod 10 = 9 \mod 10$$

So the ones’-place digit of $3^{714}$ is 9.
Factoring by algebraic identities

Trial division does not scale upward well. All methods for factoring integers above about $10^{20}$ use other methods, most based in part on algebraic factoring.

Polynomials of the form $x^2 - 1$, $x^3 - 1$, $x^4 - 1$ have at least one systematic factorization

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \ldots + x^2 + x + 1)$$

Equivalently, polynomials like $x^2 - y^2$, $x^3 - y^3$, and $x^4 - y^4$ have factorizations

$$x^n - y^n =$$

$$(x - y)(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1})$$

For odd $n$, replacing $y$ by $-y$ gives a variant

$$x^n + y^n =$$

$$(x + y)(x^{n-1} - x^{n-2}y + \ldots - xy^{n-2} + y^{n-1})$$
For composite exponent \( n \) one obtains several different factorizations

\[
x^{30} - 1 = (x^{15})^2 - 1 = (x^{15} - 1)(x^{15} + 1)
\]
\[
x^{30} - 1 = (x^{10})^3 - 1 = (x^{10} - 1)(x^{20} + x^{10} + 1)
\]
\[
x^{30} - 1 = (x^{6})^5 - 1 = (x^{6} - 1)((x^{6})^4 + \ldots + 1)
\]
\[
x^{30} - 1 = (x^{5})^6 - 1 = (x^{5} - 1)((x^{5})^5 + \ldots + 1)
\]
\[
x^{30} - 1 = (x^{3})^{10} - 1 = (x^{3} - 1)((x^{3})^9 + \ldots + 1)
\]
\[
x^{30} - 1 = (x^{2})^{15} - 1 = (x^{2} - 1)((x^{2})^{14} + \ldots + 1)
\]
in addition to the basic

\[
x^{30} - 1 = (x - 1)(x^{29} + \ldots + 1)
\]
Such *algebraic* factorizations yield *numerical* partial factorizations of some special large numbers, such as
\[ 2^{33} - 1 = (2^{11})^3 - 1 = (2^{11} - 1)(2^{22} + 2^{11} + 1) \]
\[ 2^{33} - 1 = (2^3)^{11} - 1 = (2^3 - 1)(2^{30} + \ldots + 1) \]
Thus, \( 2^{33} - 1 \) has factors \( 2^3 - 1 = 7 \) and \( 2^{11} - 1 = 23 \cdot 89 \). It is then easier to complete the *prime* factorization
\[ 2^{33} - 1 = 7 \cdot 23 \cdot 89 \cdot 599479 \]

Note that
\[ 1 < 2^{11} - 1 < 2^{33} - 1 \]
which assures that \( 2^{11} - 1 \) is a *proper* factor of \( 2^{33} - 1 \).

In this case the largish number 599479 might be awkward to understand. A little later we can see how to more efficiently factor or prove prime a special number such as 599479. (It is prime.)
As another example, to start to factor $5^{10} - 1 = 9765624$ use

$$5^{10} - 1 = (5^2)^5 - 1$$

$$= (5^2 - 1)((5^2)^4 + (5^2)^3 + \ldots + 5^2 + 1)$$

$$5^{10} - 1 = (5^5)^2 - 1 = (5^5 - 1)(5^5 + 1)$$

So $5^2 - 1 = 24$ and $5^5 - 1 = 3124$ (and $5^5 + 1 = 3126$) are factors. By Euclid, $\gcd(24, 3124)$ is 4, and $3124/4 = 781$ is readily factored into primes by trial division as $11 \cdot 71$. Since $24/4 = 6$ and $11 \cdot 71$ are relatively prime and both divide 9765624, their product also divides it, and

$$\frac{9765624}{4 \cdot 6 \cdot 11 \cdot 71} = \frac{3126}{6} = 521$$

Trial division shows that 521 is prime, so

$$5^{10} - 1 = 2^3 \cdot 3 \cdot 11 \cdot 71 \cdot 521$$

(Tedious to check 521? 781? See below...)
Another algebraic emulation of numerical methods involves thinking in terms of the Euclidean algorithm and its effect on numbers of special forms like $2^n - 1$.

**Theorem:** For any integers $a, b$ with $\gcd(a, b) = 1$ and for positive integers $m, n$

$$\gcd(a^m - b^m, a^n - b^n) = a^{\gcd(m, n)} - b^{\gcd(m, n)}$$

This is often invoked where $b = 1$, so

$$\gcd(a^m - 1, a^n - 1) = a^{\gcd(m, n)} - 1$$

For example,

$$\gcd(2^{105} - 1, 2^{140} - 1) = 2^{\gcd(105, 140)} - 1$$

$$= 2^{35} - 1$$
Proof: We’ll just give the proof in the simpler case that $b = 1$. Suppose $m < n$, and suppose that $d$ divides both $a^n - 1$ and $a^m - 1$. Then $d$ divides

$$(a^n - 1) - a^{n-m}(a^m - 1) = a^{n-m} - 1$$

And we can go back: if $d$ divides both $a^{n-m} - 1$ and $a^m - 1$ then $d$ divides $a^n - 1$.

If $n - m \geq m$ this step can be repeated. Eventually, we’ll find that if $d$ divides $a^n - 1$ and $a^m - 1$, then $d$ divides $a^{n-qm} - 1$ with $n - qm < m$. And if $d$ divides $a^m - 1$ and $a^{n-qm} - 1$ then it divides $a^n - 1$. This is like a single step of the Euclidean algorithm applied to $n, m$.

Filling this out gives the results...

///
Fermat-Euler shortcut

Above, one might worry that in

\[ 2^{33} - 1 = 7 \cdot 23 \cdot 89 \cdot 599479 \]

the large number 599479 remains.

**Theorem:** (Fermat, Euler) A prime factor \( p \) of \( b^n - 1 \) either divides \( b^d - 1 \) for a divisor \( d < n \) of the exponent \( n \), or else \( p = 1 \mod n \).

Since here the exponent 33 is odd, and since primes bigger than 2 are odd, in fact we can say that if a prime \( p \) divides \( 2^{33} - 1 \) and is not 7, 23, 89, then \( p = 1 \mod 66 \).

Thus, in testing 599479 by trial division by \( D \leq \sqrt{599479} \sim 774 \) we do not test all odd numbers, but only 67, 133, 199, \ldots and only need to do

\[ \sqrt{599479}/66 \sim 11 \]

trial divisions to see that 599479 is prime.
In the smaller example $5^{10} - 1 = 9765624$ we easily found proper factors

$$5^5 - 1 = 3124 \quad 5^2 - 1 = 24$$

(and $3126 = 5^5 + 1 = (5 + 1)(5^4 - \ldots + 1)$). As before

$$976524 = 4 \cdot \frac{3124}{4} \cdot 6 \cdot \frac{3126}{6}$$

$$= 4 \cdot 781 \cdot 6 \cdot 521$$

The Fermat-Euler trick says that any prime factor of $5^5 - 1 = 4 \cdot 781$ not already appearing in $5^d - 1$ for $d\mid 5$ and $d < 5$ is $= 1 \mod 10$. $5^1 - 1$ is relatively prime to $781$ (Euclid). Thus, we need only look among 11 (not 21, it’s not prime), 31, … but already 31 is above $\sqrt{781}$, so if $781$ is not prime it is divisible by 11, which is so: $781 = 11 \cdot 71$. The same idea applies further: if 71 were not prime it would be divisible only by primes $= 1 \mod 10$, but $11 > \sqrt{71}$. 
Similarly, if the factor 521 of the factor $(5^5 + 1)/(5 + 1)$ of $5^{10} - 1$ were not prime it would be divisible either by

a prime dividing $5^5 - 1$ (11 and 71) or $5^2 - 1$ or $5^1 - 1$,

or by a prime $= 1 \mod 10$.

Any common factor of $5^5 + 1$ and $5^5 - 1$ divides their difference, namely 2, which does not divide 521. The only odd factor of $24 = 5^2 - 1$ is 3, which does not divide 521.

Thus, we look at primes $= 1 \mod 10$. Not 11, it divides $5^5 - 1$. Not 21, it’s not prime. 31 is prime but $> \sqrt{521}$. Thus, without really computing, 521 is prime.
By these algebra identities, $2^n - 1$ is definitely not prime unless the exponent $n$ is prime. For $p$ prime, if $2^p - 1$ is prime, it is Mersenne prime.

Not every number of the form $2^p - 1$ is prime, even with $p$ prime. For example,

\[
2^{11} - 1 = 23 \cdot 89 \\
2^{23} - 1 = 47 \cdot 178481 \\
2^{29} - 1 = 233 \cdot 1103 \cdot 2089 \\
2^{37} - 1 = 223 \cdot 616318177 \\
2^{41} - 1 = 13367 \cdot 164511353
\]

Nevertheless, usually the largest known prime at any moment is a Mersenne prime, such as

\[2^{6972593} - 1\]

**Theorem (Lucas-Lehmer)** Let $L_0 = 4$, $L_n = L_{n-1}^2 - 2$. For $p$ an odd prime, $2^p - 1$ is prime if and only if

\[L_{p-2} = 0 \mod 2^p - 1\]
Not every algebraic factorization really gives a proper numerical factorization. For example,

\[ n^2 - 1 = (n - 1)(n + 1) \]

yet with \( n = 2 \) we have

\[ 2^2 - 1 = 3 = \text{prime} \]

The point is to check that the algebraic factors give proper numerical factors. Here, solving

\[ n - 1 > 1 \quad n + 1 > 1 \]

for integers \( n \) we get \( n > 2 \). Thus, for \( n > 2 \) the value of \( n^2 - 1 \) is definitely composite, because each of the algebraic factors \( n - 1 \) and \( n + 1 \) is greater than 1 (and, thus, necessarily less than \( n^2 - 1 \)).
The algebraic factorization

\[ n^2 + 7n + 12 = (n + 3)(n + 4) \]

shows that \( n^2 + 7n + 12 \) is composite when both \( n + 3 > 1 \) and \( n + 4 > 1 \), that is, for \( n > -2 \).

By contrast, for example when \( n = -2 \)

\[ (-2)^2 + 7(-2) + 12 = (-2 + 3)(-2 + 4) = 2 \]

which is prime.
Fermat’s Little Theorem

A fundamental and non-obvious fact about integers modulo a prime $p$.

**Theorem:** (Fermat’s Little Theorem) For $p$ prime for any integer $b$ we have $b^p = b \mod p$.

**Theorem:** (Variant) For $p$ prime for an integer $b$ not divisible by $p$ we have $b^{p-1} = 1 \mod p$.

**Remark:** Notice that this is very different from a possible naive expectation. Modulo $p$, an exponent of $p$ cannot be replaced by 0, despite the fact that $p = 0 \mod p$. That is, generally

$$b^p \neq b^0 \mod p$$

Instead, the variant version asserts that, for $b$ prime to $p$,

$$b^{p-1} = 1 = b^0 \mod p$$
Proof: Proven by induction on \( b \), using

\[
(b + 1)^p = b^p + \binom{p}{1} b^{p-1} + \ldots + \binom{p}{p-1} b + 1
\]

Those binomial coefficients are integers since they are the inner coefficients in

\[
(x + y)^p = x^p + \ldots + y^p
\]

On the other hand all these binomial coefficients are divisible by \( p \) since

\[
\binom{p}{i} = \frac{p!}{i! (p - i)!}
\]

and the denominator has no factor of \( p \). (Unique Factorization!) Thus, we have

\[
(b + 1)^p = b^p + 1 = b + 1 \mod p
\]

by induction. //
The factorizations of $x^n - 1$ above are **cyclotomic** factorizations. Less well known are **Lucas-Aurifeullian-LeLasseur** factorizations

$$x^4 + 4 = (x^4 + 4x^2 + 4) - (2x)^2$$
$$= (x^2 + 2x + 2)(x^2 - 2x + 2)$$

More exotic are

$$\frac{x^6 + 27}{x^2 + 3} = (x^2 + 3x + 3)(x^2 - 3x + 3)$$

$$\frac{x^{10} - 5^5}{x^2 - 5} =$$

$$(x^4 + 5x^3 + 15x^2 + 25x + 25)$$
$$\times (x^4 - 5x^3 + 15x^2 - 25x + 25)$$

and

$$\frac{x^{12} + 6^6}{x^4 + 36} =$$

$$(x^4 + 6x^3 + 18x + 36x + 36)$$
$$\times (x^4 - 6x^3 + 18x - 36x + 36)$$
and further

\[
\frac{x^{14} + 7^7}{x^2 + 7} = \]

\[
(x^6 + 7x^5 + 21x^4 + 49x^3 + 147x^2 + 343x + 343)
\times(x^6 - 7x^5 + 21x^4 - 49x^3 + 147x^2 - 343x + 343)
\]

These Aurifeuilllian factorizations yield further factorizations of special large numbers, such as

\[
2^{22} + 1 = 4 \cdot (2^5)^4 + 1
\]

\[
= (2(2^5)^2 + 2(2^5) + 1)(2(2^5)^2 - 2(2^5) + 1)
\]

\[
= 2113 \cdot 1985 = 2113 \cdot 5 \cdot 397
\]

and similarly

\[
\frac{3^{33} + 1}{3^{11} + 1} = \frac{27 \cdot (3^5)^6 + 1}{3 \cdot (3^5)^2 + 1}
\]

\[
= (3(3^5)^2 + 3(3^5) + 1)(3(3^5)^2 + 3(3^5) + 1)
\]

\[
= 7 \cdot 25411 \cdot 176419
\]