Primes, modular arithmetic

Proposition 1.6.19 Let $p \in \mathbb{N}$ be prime, let a, b be nonzero integers. If $p|ab$ then $p|a$ or $p|b$.

Proof Since p is prime $\gcd(p,a) = 1$ or p.
if $\gcd(p,a) = p$ then $p|a$ and we are done.
if $\gcd(p,a) = 1$, then we can find integers s, t such that

$$1 = ps + at$$

then $b = bps + abt$ (multiply by b)
We know $p|ab$, so $p|abt$, and obviously $p|bps$, so we conclude $p|b = bps + abt$. $\blacksquare$

Theorem 1.6.21 Prime factorization of n is unique (up to order of the factors).

Proof Strong induction on n. Base case $n=1$: only empty product is possible.
Suppose for every $m < n$, prime factorization is unique.
Suppose $n = p_1 \cdots p_k = q_1 \cdots q_\ell$ are two prime factorizations.

We may reorder the factors so that

$$p_1 \le p_2 \le \cdots \le p_k \qquad q_1 \le q_2 \le \cdots \le q_\ell .$$

Suppose $p_1 \le q_1$ (if not, swap names of p's and q's)

Since $p_1 | n = q_1 \cdots q_\ell$, we have that $p_1 | q_j$ for some j, $1 \le j \le \ell$
Since p_1 and q_j are prime, $p_1 = q_j$.

Then $p_1 \le q_1 \le q_j = p_1$ so $p_1 = q_1 = q_j$.

Then take $m = \frac{n}{p_1} = \frac{n}{q_1} = p_2 \cdots p_k = q_2 \cdots q_\ell$

since $m < n$, we apply induction hypotheses to conclude $k = \ell$ and $p_i = q_i$ for $2 \le i \le k$. Thus the two factorizations of n are not actually different. $\boxtimes$

Modular arithmetic (Clock arithmetic = mod 12)

Definition Let $a, b, n \in \mathbb{Z}$, $n \ge 1$. We say
"a is congruent to b modulo n"
$a \equiv b \pmod{n}$ if $n \mid (b-a)$.

- Observe: given $a \in \mathbb{Z}$ and $n \ge 1$, we can apply long division to get $q, r \in \mathbb{Z}$ with $a = qn + r$ and $0 \le r < n$

Then $a - r = qn$ is divisible by n, so $r \equiv a \pmod{n}$
"Any number a is congruent modulo n to the remainder of a divided by n."

Integer arithmetic works well with congruence:
Lemma 1.7.5: Let $a, a, b, b' \in \mathbb{Z}$. Assume $a \equiv a' \pmod{n}$, $b \equiv b' \pmod{n}$.
then $a + b \equiv a' + b' \pmod{n}$ and $ab \equiv a'b' \pmod{n}$.

Proof Know $n \mid (a-a')$ and $n \mid (b-b')$, so
$n \mid (a-a') + (b-b') = (a+b) - (a'+b')$
so $(a+b) \equiv (a'+b') \bmod n$.

Also $n \mid (a-a')b + a'(b-b') = (ab - a'b + a'b - a'b') = ab - a'b'$
so $ab \equiv a'b' \pmod n$ ▨

<u>Example</u> Compute $(7964)\cdot(11203) \bmod 10$.
since $7964 \equiv 4 \bmod 10$,
$11203 \equiv 3 \bmod 10$,
we have $7964 \cdot 11203 \equiv 4 \cdot 3 = 12 \equiv 2 \bmod 10$

<u>Note</u>: $n \mid a \iff a \equiv 0 \bmod n$.

<u>Fact</u>: $3 \mid a \iff 3 \mid (\text{sum of digits of } a)$ write $a = \sum_{j=0}^{k} a_j 10^j$

where $a_j \in \{0, 1, \dots, 9\}$ are digits of a.
Since $10 \equiv 1 \bmod 3$, we have $10^j \equiv 1^j = 1 \bmod 3$.
So
$$a = \sum_{j=0}^{k} a_j 10^j \equiv \sum_{j=0}^{k} a_j \cdot 1^j = \sum_{j=0}^{k} a_j \pmod 3$$
so $a \equiv 0 \bmod 3 \iff \sum_{j=0}^{k} a_j \equiv 0 \pmod 3$.

The relation of congruence (i.e. the concept "is congruent to") is the canonical first example of an <u>equivalence relation</u>.

<u>Lemma 1.7.2</u> For $a, b, c, n \in \mathbb{Z}$, $n \geq 1$, we have
(i) $a \equiv a \pmod n$ (reflexive)
(ii) $a \equiv b \pmod n$ iff $b \equiv a \pmod n$ (symmetric)
(iii) if $a \equiv b \pmod n$ and $b \equiv c \pmod n$ then $a \equiv c \pmod n$ (transitive)

<u>Proof</u> (i) $a - a = 0$ and $n \mid 0$ (ii) since $b - a = -(a-b)$, $n \mid b-a \iff n \mid a-b$. (iii) $n \mid b-a$ and $n \mid c-b \Rightarrow n \mid (c-b)+(b-a) = c-a$.

<u>Definition</u> Fix $n \in \mathbb{N}$. For $a \in \mathbb{Z}$, the <u>congruence class</u> of a modulo n is the set

$$[a] = \{ b \in \mathbb{Z} \mid b \equiv a \bmod n \} = \{ a + kn \mid k \in \mathbb{Z} \}$$

To emphasize the dependence on n we write $[a]_n$.

<u>Lemma 1.7.3</u> Fix $n \in \mathbb{Z}$. For $a, b \in \mathbb{Z}$, the following are equivalent.
(i) $a \equiv b \mod n$
(ii) $[a] = [b]$
(iii) $\mathrm{rem}_n(a) = \mathrm{rem}_n(b)$ (rem_n = remainder upon div. by n.)
(iv) $[a] \cap [b] \neq \emptyset$.

<u>Proof</u> Goodman.

<u>Corollary 1.7.4</u> There are exactly n distinct congruence classes mod n namely $[0], [1], [2], \ldots, [n-1]$. These sets are pairwise disjoint.

Denote the set of congruence classes

$$\mathbb{Z}_n = \{ [0], [1], \ldots, [n-1] \}$$

We wish to define $+$ and $\cdot$ in $\mathbb{Z}_n$ by the formulas

$$[a] + [b] = [a+b] \quad \text{and} \quad [a] \cdot [b] = [a \cdot b]$$

This works, but it is worth thinking about why it works. The issue is that the object denoted $[a]$ could be represented other ways, for instance as $[a']$ where $a \equiv a' \mod n$. But then $a+b$ would become $a'+b$ which is different....

The crucial point is this: if $[a]=[a']$ and $[b]=[b']$, then $[a+b]=[a'+b']$ and $[a\cdot b]=[a'\cdot b']$.
This follows from Lemmas 1.7.3 and 1.7.5.

We say that addition and multiplication of congruence classes is "well-defined". This is a logical pattern that will repeat whenever we try to define a function that seems to depend on a choice of representative element.

Proposition 1.7.7 The operations $+$ and $\cdot$ on $\mathbb{Z}_n$ satisfy commutative law, associative law, distributive law.
$[0]$ is additive identity, $[1]$ is multiplicative identity
The additive inverse of $[a]$ is $[-a]$ (or $[n-a]$).