Corollary: If $\gcd(a,b)$ exists $\forall\, a,b \in M$, then every irreducible element is prime.

proof: Let p be an irreducible element $\notin M^\times$.

To prove $p \mid bc \implies p \mid b$ or $p \mid c$.

$p = \gcd(bc, p) \implies \gcd(b,p) = p$ or $\gcd(c,p) = p$.

because: If $\gcd(b,p) = 1$ i.e $p \nmid b$, then by lemma 5.1 $p \mid c$.

Proof of Theorem 5.3: Since existence of gcd implies that every irreducible element is a prime, M becomes a factorial monoid.

Division Algorithm, & Euclidean Algorithm

L 6|1

Divison algorithm for finding gcd: Let $a, b \in \mathbb{Z}$, then there exists unique integers q, r such that $a = qb + r$ with $0 \le r < |b|$

Proof: We may assume $b > 0$, $a \ge 0$. We prove the existence by induction on a

if $a = 0$, $q = r = 0$

If hypothesis is true for ~~$a < b$~~, $a < n$,

then ~~$a \ge b$~~ when $a = n$, $a - b < n$.

Therefore, from hypothesis $a - b = \tilde{q}\, b + \tilde{r}$ $\tilde{q} \in \mathbb{Z}$, $0 \le \tilde{r} < b$

$a - b = \tilde{q}\, b + \tilde{r} \implies a = (\tilde{q}+1)\, b + \tilde{r}$. $(\tilde{q}+1) \in \mathbb{Z}$

To prove uniqueness, let $a = qb + r = q'b + r'$

$\implies 0 = (q - q')b + (r - r')$

$\implies (q - q')b = (r' - r)$ ⇗

But $r' - r < |b|$ ⇗ $q = q'$ and $r = r'$.

$\implies r' - r = 0$ ⇗

Gauss bracket: Let $b \in \mathbb{N}^*$, $a \in \mathbb{N}$, ~~then~~

$$\frac{a}{b} = q + \frac{r}{b}, \quad 0 \leq r < 1.$$

$\left[\frac{a}{b}\right] = q$ is called the Gauss bracket: the integral part of $\frac{a}{b}$.

Example: g-adic expansion of $g \geq 2$, $g \in \mathbb{N}^*$

For every $n \in \mathbb{N}$, $\exists\ r, a_0, a_1, \ldots a_r$ with $a_r \neq 0$, $0 \leq a_i < g$ $\forall i$, such that

$$n = a_0 + a_1 g + a_2 g^2 \ldots a_r g^r$$

The r and $\{a_i\}$ are unique. The g-adic expansion is also denoted as $n = (a_r a_{r-1} \ldots a_0)_g$, and $a_0, a_1, a_2 \ldots a_r$ are the digits in the expansion.

Existence of the g-adic expansion:

Let $q_0 = n$. $\quad q_0 = q_1 g + a_0 \quad 0 \leq a_0 < g$.

$$q_0 = (q_2 g + a_1) g + a_0 \quad 0 \leq a_1 < g$$

$$= q_2 g^2 + a_1 g + a_0$$

Again expand q_2 $\quad q_0 = (q_3 g + a_2) g^2 + a_1 g + a_0$

. . . . . .

At each successive stage $q_k < q_{k-1}$, and after finite number of steps, this process must stop.

Euclidean Algorithm for finding gcd:

Let $a, b \in \mathbb{Z}$, $b \neq 0$, let $r_0 = a$, $r_1 = b$

$r_0 = q_1 r_1 + r_2$ where $0 \leq r_2 < r_1$, $q_1 \in \mathbb{Z}$

If $r_2 \neq 0$, $r_1 = q_2 r_2 + r_3$. If $r_3 = 0$, stop, else expand r_2 in terms of r_3... Generally, $r_{i-1} = q_i r_i + r_{i+1}$.

Continuing this process, $r_{k-1} = q_k r_k + r_{k+1}$, $r_k = q_{k+1} r_{k+1}$

The gcd of (a, b) is r_{k+1}.

Proof: (Outline.) Verify that for every $i = 1, 2 \ldots k$, if $\gcd(r_i, r_{i+1})$ exists then $\gcd(r_{i-1}, r_i)$ also exists, and they are equal.

Bezout's lemma: $a, b \in \mathbb{N}$, $b \neq 0$, then $\gcd(a,b) = sa + tb$ where $s, t \in \mathbb{Z}$. If $\gcd(a,b) = 1$, then $sa + tb = 1$. In this case a, b are relatively prime.

$r_i = s_i a + t_i b \qquad s_i, t_i \in \mathbb{Z}$

$s_0 = 1, \; t_0 = 0, \quad s_1 = 0, \; t_1 = 1$, for each $i = 0, \ldots k+1$.

$s_{i+1} = s_{i-1} - q_i s_i, \quad t_{i+1} = t_{i-1} - q_i t_i$

Example: $a = 366617, \quad b = 12247$

i	0	1	2	3	4
q_i		2	1	164	2
s_i	1	0	1	-1	165
t_i	0	1	-2	3	-3×164

Lemma: If $p \in \mathbb{N}_*$ is irreducible and $p \mid ab$ then either $p \mid a$ or $p \mid b$. In other words all irreducible numbers are prime in $\mathbb{N}^*$.