Chapter 1, part 5

Primes

Every non-zero integer a is divisible by $1, -1, a, -a$

Prime "has no extra divisors"

Def $p \in \mathbb{Z}$ is a prime if $p \neq 0$, $p \neq \pm 1$, and p has no divisors besides ± 1 and $\pm p$.

If p is a prime, then so is $-p$ (because they have same set of divisors).

Primes cannot divide each other. If p and q are primes and $p \mid q$, then $p = \pm q$.

Recall Th 1.4 If $a \mid bc$ and $(a,b)=1$ then $a \mid c$.

Let p be a prime, $p \mid bc$.

Cases:

$p \mid b$ (implies $p \mid bc$ because $b = ps$, thus $bc = psc$)

$p \nmid b$ implies $(p, b) = 1$

Th 1.5 Let p be an integer, $p \neq 0$, $p \neq \pm 1$.

Then p is a prime iff it has the following property:

$p \mid bc$ implies $p \mid b$ or $p \mid c$ (or both)

Pf Let p be a prime. Assume that $p \mid bc$, and $p \nmid b$.

Then $(p,b)=1$, and, by Th 1.4, $p|c$.

Converse (Ex 14)

Counterpositive: If p is not a prime then p does not satisfy the property.

Suffices to find b and c such that $p|bc$ but $p\nmid b$ and $p\nmid c$.

Let $b|p$ and $\underline{\underline{b\neq\pm 1}}$, $\underline{b\neq\pm p}$.

$p=bc$ Wanted: $p\nmid b$ and $p\nmid c$ | $p=bc$ means $p=bc\cdot 1$, $p|bc$

If $p|b$ then $b=pz$

$p=pzc$

$1=zc$ implies $|z|\cdot|c|=1$ implies $|z|=1$ and $|c|=1$.

In particular $c=\pm 1$ implies $\underline{b=\pm p}$. Thus $p\nmid b$.

If $p|c$ then $c=py$

$p=bpy$

$1=by$ implies $|b||y|=1$ implies $|b|=1$ and $|y|=1$

In particular $\underline{\underline{b=\pm 1}}$.