MATH 407
2/19/18

Relative primality and prime:

Def. $a,b \in \mathbb{Z}$ are relatively prime iff $\gcd(a,b)=1$
iff $1 = na+mb$, some $m,n \in \mathbb{Z}$

Prop. 1.2.3 : $a,b,c \in \mathbb{Z}$, $|a|+|b| \neq 0$
a) if $b \mid ac$, then $b \mid (a,b)c$
b) if, in addition, $(a,b)=1$, then $b \mid c$
c) if $b \mid a$ and $c \mid a$ and $(b,c)=1$, then $(bc) \mid a$
d) $(a,bc)=1$ iff $(a,b)=1$ and $(a,c)=1$

* Note: notation $(x,y) := GCD(x,y)$

Pf.: a) $(a,b) = na+mb$, $b \mid (ac)$

$$(a,b)c = (na+mb)c$$
$$= n(ac) + (mc)b$$

b) Part b) of Prop. 1.2.3 is a corollary

c) $b \mid a$ so $a = bq$ for some $q \in \mathbb{Z}$
$c \mid a$ so $c \mid bq$
$\because (c,b)=1$, part b) gives $c \mid q$

$q = cq_1$ for some q_1

Thus, $a = b(cq_1)$
$= (bc)q_1$
$\therefore (bc) \mid a$

d) $(a,bc)=1$
If $d=(a,b)$, then $d \mid a$ and $d \mid b$

(contd. $\rightarrow$)

So, $d \mid bc$

Thus, $d \mid (a, bc) = 1$

$d = 1$

$\therefore (a, bc) = 1$ if $(a,b) = 1$ and $(a,c) = 1$

Conversely,

$(a,b) = 1, \; na + mb = 1, \; n, m \in \mathbb{Z}$

$(a,c) = 1, \; la + kc = 1, \; l, k \in \mathbb{Z}$

$(na + mb)(la + kc) = (1)(1)$

$\Rightarrow (nla^2 + nkac + mlab + (mk)(bc)) = 1$

$\Rightarrow a(nla + nkc + mlb) + (bc)(mk) = 1$

<u>Def.</u>: $p > 1$ is prime iff $d \in \mathbb{N}$, $d \mid p$ implies $d \in \{1, p\}$

<u>Lemma</u>: p is prime iff there exists no divisor $1 < d < p$

p is prime iff $p = ab$, $a > 1$, $b > 1$ (impossible)

<u>Lemma</u>: $p > 1$ is prime iff $p \mid ab$ implies $p \mid a$ or $p \mid b$

<u>Pf.</u> If $(p, a) = p$, then $p \mid a$. Done.

Else, $(p, a) = 1$. Part b) of Prop. 1.2.3 implies $p \mid b$.

<u>Corr.</u>: If p is prime and $p \mid \prod_{i=1}^{n} a_i = (a_1 \ldots a_n)$,

then $p \mid a_i$ for some i

$$p \,\Big|\, \prod_{i=1}^{n+1} a_i \Rightarrow p \,\Big|\, \left(\prod_{i=1}^{n} a_i\right) \cdot a_{n+1}$$

Either $p \,\Big|\, \prod_{i=1}^{n} a_i$ or $p \mid a_{n+1}$

<u>Lemma:</u> Any $a \in \mathbb{N} \setminus \{1\}$ has a prime factor.

<u>Pf.</u> Let $D \subseteq \mathbb{N}$ be all divisors of a larger than 1.
$D \neq \emptyset$ since $a \in D$
Let $p = \min(D) > 1$
$p \mid a$ and p is prime
If $1 < d < p$ and $d \mid p$ then $d \in D$
But $d < p = \min(D) > 1$ (contradiction)