Tom Leighton and Ankur Moitra

Some useful facts about divisibility and modulo arithmetic

Divisibility

D1. If $a \mid b$ and $b \mid c$, then $a \mid c$.

D2. If $a \mid b$ and $a \mid c$, then $a \mid sb + tc$ for all s and t.

D3. For all $c \neq 0$, $a \mid b$ if and only if $ca \mid cb$.

Greatest common divisor

G1. $\gcd(ka, kb) = k \cdot \gcd(a, b)$ for all $k > 0$.

G2. If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.

G3. If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

G4. If $m \mid a$ and $m \mid b$, then $m \mid \gcd(a, b)$.

Modulo arithmetic

M1. $a \equiv a \pmod{n}$

M2. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$

M3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ implies $a \equiv c \pmod{n}$

M4. $a \equiv b \pmod{n}$ implies $a + c \equiv b + c \pmod{n}$

M5. $a \equiv b \pmod{n}$ implies $ac \equiv bc \pmod{n}$

M6. $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ imply $a + c \equiv b + d \pmod{n}$

M7. $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ imply $ac \equiv bd \pmod{n}$

Warning: it is *not* the case that $ak \equiv bk \pmod{n}$ implies $a \equiv b \pmod{n}$ in general. It *is* true however if $\gcd(n, k) = 1$; in particular, if n is prime and k is not a multiple of n.