6.042/18.062J Mathematics for Computer Science — September 22, 2016
Tom Leighton and Ankur Moitra

Some useful facts about Modular 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.