1. Mod Madness

① 1. $a\in\mathbb{Z}$ $b\in\mathbb{Z}$ $c\in\mathbb{Z}$ $m\in\mathbb{Z}$ $c>0$ $m>0$ given

1.1 $a\equiv b \pmod m$ Assumption

1.2 $m \mid (a-b)$ Congruency: 1.1

1.3 $\exists k\in\mathbb{Z}$ that $a-b=km$ Divisibility: 1.2

1.4 $c(a-b)=ckm$, $ca-cb=c\cdot km$ Algorithm: 1.1.3

1.5 $\exists k\in\mathbb{Z}$ that $ca-cb=k\cdot cm$ Intro $\exists$: 1.4

1.6 $cm \mid ca-cb$ Divisibility: 1.5

1.7 $ca\equiv cb \pmod{cm}$ Congruency: 1.6

2. $a\equiv b\pmod m \rightarrow ca\equiv cb \pmod{cm}$ Direct proof rule

② 1. $a\in\mathbb{Z}$ $b\in\mathbb{Z}$ $c\in\mathbb{Z}$ $m\in\mathbb{Z}$ $c>0$ $m>0$ given

1.1 $ca\equiv cb \pmod{cm}$ Assumption

1.2 $cm \mid (ca-cb)$ Congruency: 1.1

1.3 $\exists k\in\mathbb{Z}$ that $ca-cb=kcm$ Divisibility: 1.2

1.4 $a-b=km$ Algorithm: 1.1.3

1.5 $\exists k\in\mathbb{Z}$ that $a-b=km$ Intro $\exists$: 1.4

1.6 $m \mid a-b$ divisibility: 1.5

1.7 $a\equiv b \pmod m$ Congruency: 1.6

2. $ca\equiv cb\pmod{cm} \rightarrow a\equiv b \pmod m$ Direct proof rule

$\Downarrow$ (bicondition law)

$\therefore$ $ca\equiv cb \pmod{cm} \leftrightarrow a\equiv b\pmod m$

$\Rightarrow$ $\therefore$ for any integer a and b and any positive integer c and m. $ca\equiv cb \pmod{cm}$ if and only if $a\equiv b\pmod m$

2. GCDs are easier than factoring

(a) $\gcd(0,12^{73}) = 12^{73}$

(b) $\gcd(139,69)$

$=\gcd(69, 139 \bmod 69)$

$=\gcd(69,1)$

$=\gcd(1, 69 \bmod 1)$

$=\gcd(1,0)$

$=1$

(c) $\gcd(91,434)$

$=\gcd(91, 434 \bmod 91) = \gcd(91,70)$

$=\gcd(70, 91 \bmod 70) = \gcd(70,21)$

$=\gcd(21, 70 \bmod 21) = \gcd(21,7)$

$=\gcd(7, 21 \bmod 7) = \gcd(7,0)$

$=7$