Solutions for homework problems

1.3. If $p>3$ is a prime, either $p+2$ or $p+4$ is not a prime.

Proof. If $p>3$, $p\equiv 1$ or $2 \pmod 3$.

If $p\equiv 1 \pmod 3$, $p+2\equiv 0 \pmod 3$

If $p\equiv 2 \pmod 3$, $p+4\equiv 0 \pmod 3$.

3.2. (a) $\left(\frac{m^2-2m-1}{m^2+1}, \frac{-m^2-2m+1}{m^2+1}\right)$

(b) There are no rational points on $x^2+y^2=3$.

Proof. If (x,y) is a rational point,

$x=\frac{a}{c}$, $y=\frac{b}{c}$, $\gcd(a,b,c)=1$.

Then $a^2+b^2=3c^2$.

Note that if $a\in\mathbb{Z}$, $a^2\equiv 0$ or $1 \pmod 4$.

So $a^2+b^2\equiv 0,1,2 \pmod 4$

$3c^2\equiv 0,3 \pmod 4$

Hence a,b,c are all even

Contradiction.

3.3. $\left(\frac{1+m^2}{1-m^2}, \frac{2m}{1-m^2}\right)$, $m\neq\pm 1$

and $(-1,0)$

3.4. The line through two points $(1,-3)$ and $\left(-\frac{7}{4}, \frac{13}{8}\right)$ is

$$y=-\frac{37}{22}x-\frac{29}{22}$$

Solving together with $y^2=x^3+8$, we have

$$x^3+8=\left(\frac{37}{22}x+\frac{29}{22}\right)^2$$

Since $x=1, -\frac{7}{4}$ are solutions, it factors as $(x-1)(x+\frac{7}{4})(x-\square)=0$.

So $\square\times\frac{7}{4}=\frac{3031}{484} \Rightarrow \square=\frac{433}{121}$.

The 3rd point is $\left(\frac{433}{121}, -\frac{9765}{1331}\right)$

5.3 $a=bq_0+r_1$, $0<r_1<b$

$b=r_1q_1+r_2$, $0<r_2<r_1$

$\vdots$

$r_{n-3}=r_{n-2}q_{n-2}+r_{n-1}$, $0<r_{n-1}<r_{n-2}$

$r_{n-2}=r_{n-1}q_{n-1}+r_n$, $0<r_n<r_{n-1}$

$r_{n-1}=r_nq_n$

$r_2=b-r_1q_1<b-q_1r_2 \Rightarrow (1+q_1)r_2<b$.

Since $q_1\geq 1$, $2r_2<b \Rightarrow r_2<\frac{1}{2}b$

Since $0<r_3<r_2$, $r_3=r_1-q_2r_2<r_1-q_2r_3$

$2r_3\leq(1+q_2)r_3<r_1$

So $r_3<\frac{1}{2}r_1$

Hence we have
$$\begin{aligned}
r_2&<\tfrac{1}{2}r_0\\
r_3&<\tfrac{1}{2}r_1\\
r_4&<\tfrac{1}{2}r_2\\
&\ \vdots\\
r_{n-1}&<\tfrac{1}{2}r_{n-3}\\
r_n&<\tfrac{1}{2}r_{n-2}\\
\hline
r_nr_{n-1}&<\left(\tfrac{1}{2}\right)^{n-1}r_0r_1
\end{aligned}$$

Since $r_n<r_{n-1}$,

$1\leq r_n^2<r_nr_{n-1}<\left(\frac{1}{2}\right)^{n-1}r_0r_1<\left(\frac{1}{2}\right)^{n-1}b^2$

Since $r_{n-1}\geq 2$, $\left(\frac{1}{2}\right)^{n-1}b^2\geq 2 \Rightarrow b^2\geq 2^n$.

5.4 (2) $LCM(m,n)\gcd(m,n) = mn$

(3) We prove that $L = \frac{mn}{g}$, $g = \gcd(m,n)$ is the least common multiple of m, n.

Since $g|m, g|n$, $L = m\left(\frac{n}{g}\right) = n\left(\frac{m}{g}\right)$ is a multiple of m and n.

Suppose K is a multiple of m and n.

$K = am = bn$.

Let $g = um + vn$

Then $K = \left(\frac{K}{g}\right)\cdot g = \frac{K}{g}\cdot(um+vn)$

$= \frac{uKm}{g} + \frac{vKn}{g} = \frac{ubmn}{g} + \frac{vamn}{g}$

$= ubL + vaL = (ub+va)L$.

Hence $L|K$.

(4) $\gcd(301337, 307829) = 541$.

So $LCM(301337, 307829) = \frac{301337 \times 307829}{541}$

$= 171460753$

(5) $m = 18a$, $n = 18b$, $\gcd(a,b) = 1$.

$720 = 18ab$. So $ab = 40 = 2^3 \times 5$.

So up to permutation, there are two possibilities $(m,n) = (720, 18)$ or $(144, 90)$.

6.2(a) Euclidean algorithm.

$105 \times (-53) + 121 \times 46 = 1$.

The general solution is

$(-53 + 121k, 46 - 105k)$

6.4(c) $155x + 341y + 385z = 1$.

$\gcd(341, 385) = 11$

$341 = 11 \times 31$, $385 = 11 \times 35$.

First, solve $155x + 11u = 1$

$x = 1 + 11k$, $u = -14 - 155k$.

Next, solve $31y' + 35z' = 1$.

$y' = -9$, $z' = +8$

Hence solutions of $31y' + 35z' = -14 - 155k$ are

$y = 9(14 + 155k) + 35l$

$z = 8(-14 - 155k) - 31l$

7.6 (a) The first 6 M-primes are

5, 9, 13, 17, 21, 29

(b) Note that if p, q are primes such that $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$, pq is an M-prime since $pq \equiv 1 \pmod 4$.

Consider $441 = 9 \times 49 = 21 \times 21$

or $693 = 9 \times 77 = 21 \times 33$

8.5 $21x \equiv 14 \pmod{91}$

$\gcd(21, 91) = 7$, $7|14$

First, solve $21u - 91v = 7$

$u = 9$, $v = 2$.

So distinct solutions are

$x = 9 \times 2 + 13k \mod 91$

$k = 0, 1, \ldots, 6$

9.1 (c) If $x \not\equiv 0 \mod 13$, $x^{12} \equiv 1 \mod 13$.

$39 = 3 \times 12 + 3$.

So $x^{39} \equiv x^3 \mod 13$.

So $x^3 \equiv 3 \mod 13$.

By computing $x \equiv -6, -5, \cdots, 5, 6$,
we can see that there is no sol.

9.2. If p is an odd prime,

$(p-1)! \equiv -1 \mod p$.

Consider $a = 1, 2, \ldots, p-1$.

Then $ax \equiv 1 \pmod p$ has a unique sol. mod p.

Consider $x^2 \equiv 1 \mod p$

$(x+1)(x-1) \equiv 0 \mod p$.

$x \equiv 1$ or $x \equiv -1 \equiv p-1 \mod p$

Therefore, for $a = 2, 3, \ldots, p-2$,
there exists $b \neq a$, $b = 2, \cdots, p-2$,
such that $ab \equiv 1 \mod p$.

Hence $(a-1)! \equiv 1 \cdot 2 \cdot \cdots \cdot (p-2)(p-1)$

$\equiv p-1 \equiv -1 \mod p$