HW 1 MME 529 Answers

1 Find the gcd of each pair using Euclid's Algorithm.

(a) $\gcd(138, 24) = 6$

$$138 = 5 \cdot 24 + 18$$
$$24 = 1 \cdot 18 + 6$$
$$18 = 6 \cdot 3$$

(b) $\gcd(414, 159) = 3$

$$414 = 2 \cdot 159 + 96$$
$$159 = 1 \cdot 96 + 63$$
$$63 = 1 \cdot 33 + 30$$
$$33 = 1 \cdot 30 + 3$$
$$30 = 10 \cdot 3$$

(c) $\gcd(1479, 272) = 17$

$$1479 = 5 \cdot 272 + 119$$
$$272 = 2 \cdot 119 + 34$$
$$119 = 3 \cdot 34 + 17$$
$$34 = 2 \cdot 17$$

(d) $\gcd(7696, 4144) = 592$

$$7696 = 1 \cdot 4144 + 3552$$
$$4144 = 1 \cdot 3552 + 592$$
$$3552 = 6 \cdot 592$$

2 Find the gcd of each pair using prime factorizations.

(a) $\gcd(138, 24) = 6$

$$\left.\begin{array}{l} 138 = 23 \cdot 3 \cdot 2 \\ 24 = 3 \cdot 2^3 \end{array}\right\} \quad 3 \cdot 2 = 6$$

(b) $\gcd(414, 159) = 3$

$$414 = 2 \cdot 3^2 \cdot 23$$
$$159 = 53 \cdot 3$$

(c) $\gcd(1479, 272) = 17$

$$1479 = 3 \cdot 17 \cdot 29$$
$$272 = 2^4 \cdot 17$$

(d) $\gcd(7696, 4144) = 592$

$$\left.\begin{array}{l} 7696 = 2^4 \cdot 13 \cdot 37 \\ 4144 = 2^4 \cdot 7 \cdot 37 \end{array}\right\} \quad 2^4 \cdot 17 = 592$$

3 (a) Prove that if $a|b$ and $a|c$, $a|(b+c)$.

Pf: $a|b \Rightarrow ak = b, \ k \in \mathbb{Z}$

$a|c \Rightarrow al = c, \ l \in \mathbb{Z}$

$\therefore \ a(k+l) = b+c$ so $a|(b+c)$.

(b) Prove $\gcd(ta, tb) = t\gcd(a,b)$

Pf: Let $d = \gcd(a,b)$. Then $d|a$ and $d|b$ and no other common divisor of a,b is greater than d. Any divisor of a,b is a divisor of ta, tb and since d is the greatest common divisor of a,b, td is the greatest common divisor of ta, tb.

$\boxed{4}$ (a) Prove that $(2n+1,\ 2n^2+2n,\ 2n^2+2n+1)$ generates Pythagorean triples.

$$(2n+1)^2 + (2n^2+2n)^2 \stackrel{?}{=} (2n^2+2n+1)^2$$

$$4n^2+4n+1 + 4n^4 + 8n^3 + 4n^2 = 4n^4 + 4n^3 + 2n^2 + 4n^3 + 4n^2 + 2n + 2n^2 + 2n + 1$$

$$4n^4 + 8n^3 + 8n^2 + 4n + 1 = 4n^4 + 8n^3 + 8n^2 + 4n + 1 \quad \checkmark$$

(b) Find a triple this formula does not generate.

$(20, 21, 29)$. Since $2n^2+2n > 2n+1$, we must assign $20 = 2n+1$, which would give the contradiction that 20 is odd. Yet $20^2 + 21^2 = 29^2$.

$\boxed{5}$ If m,n are odd integers, m^2+n^2 is even.

Pf: $m^2+n^2 = (2k+1)^2 + (2j+1)^2 = 2(2k^2+2j^2+2k+2j)$.

$\boxed{6}$

$$100 + 103 + \dots + 1399 = S$$
$$1399 + 1396 + \dots + 100 = S$$

$$1499\left(\frac{1399-100}{3} + 1\right) = 2S$$

$$325{,}283 = S$$

$\boxed{7}$

$$a + (a+d) + \dots + (a+nd) = S$$
$$a+nd + a+(n-1)d + \dots + a = S$$

$$(n+1)(2a+nd)/2 = S$$
$$\frac{n+1}{2}(a_0 + a_n) = S$$

8 Prove $\sum_{i=1}^{n} i^2 = n(n+1)(2n+1)/6$.

Pf (Induction):

$\underline{P(1)}$ $\quad 1(1+1)(2+1)/6 = 6/6 = 1 = \sum_{i=1}^{1} i^2$.

$\underline{P(n) \Rightarrow P(n+1)}$

$$\begin{aligned}
\sum_{i=1}^{n+1} i^2 &= n(n+1)(2n+1)/6 + (n+1)^2 \\
&= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} \\
&= (n+1)\left[2n^2 + 4n + 3n + 6\right]/6 \\
&= (n+1)\left[2n(n+2) + 3(n+2)\right]/6 \\
&= (n+1)(n+2)(2(n+1)+1)/6.
\end{aligned}$$

9 What are the possible values of $\gcd(n, n+2)$?

$$\gcd(n, n+2) = \begin{cases} 2, & n \text{ even} \\ 1, & n \text{ odd} \end{cases}$$

Pf: $\quad n+2 = 1 \cdot n + 2$

$\quad\quad n = 2q + r$

If n is even, $\exists\, q$ s.t. $n = 2q$ so that $r = 0$.

Then $\gcd(n+2, n) = 2$ by the E.A.

If n is odd $\exists\, q$ s.t. $n = 2q+1$.

$$\begin{aligned}
n+2 &= 1 \cdot n + 2 \\
n &= 2q + 1 \\
2 &= 1 \cdot 2
\end{aligned} \quad \rightarrow \gcd(n+2, n) = 1 \text{ by the E.A.}$$

10 (a) $S = 1 + 2 + 2^2 + \cdots + 2^{n-1}$

$2S = \quad 2 + 2^3 + \cdots + 2^n$ $\quad \rightarrow \quad S = 2S - S = 2^n - 1$.

Also, $\sum_{i=0}^{n-1} r^i = \frac{1-r^n}{1-r}$. If $r = 2$,

$$\sum_{i=0}^{n-1} 2^i = \frac{1-2^n}{1-2} = 2^n - 1$$

(b) Find the binary forms of each of the following:

$2^7 - 1 = 111111_2$, $\quad 2^9 - 1 = 111111111_2$, $\quad 2^n - 1 = \underbrace{111\ldots1}_{n \text{ 1's}}{}_2$.

11 Show how numbers of the form $2^{pq}-1$ can be factored using the geometric series,

$$2^{pq}-1 = (2^p)^q - 1 = (2^p-1)\sum_{i=0}^{q-1}(2^p)^i$$
$$= (2^p-1)(1+2^p+2^{2p}+\dots+2^{(q-1)p}).$$

12 Write Maple or Matlab code to generate Pythagorean triples.

Maple:
```
for i=1 to N do:
    print(2+i+1, 2i^2+2i, 2i^2+2i+1).
```