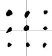
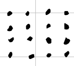
1.2. 1 $\quad 1+3=4=2^2 \quad 1+3+5=9=3^2$

$1+3+5+7=4^2$



so we have

$1+3+\cdots+2n+1$. Thus we have

Thus $1+3+\cdots+2n+1=k^2$

1.3. Consider the prime number p where we have $3 \nmid p$. Then we have $p=3k+1$ or $p=3k+2$ for some k. If $p=3k+1$ then $p+2=3k+3$, so $3 \mid (p+2)$. If $p=3k+2$ then $p+4=3k+6=3(k+2)$, so $3 \mid (p+4)$. Therefore for any p not divisible by 3 we still have $p+2$, $p+4$ to be divisible by 3. Hence such triple is finite. ∎

1, 2, 6, 7, 9

1. (a) Lemma. For any $c \in \mathbb{Z}$ we have $[c^2]_3 \neq [2]_3$.
Proof. Note that $[0^2]_3 = [0]_3$, $[1^2]_3 = [1]_3$, and $[2^2]_3 = [4]_3 = [1]_3$.

We show that either a or b is a multiple of 3.
First we consider $[a]_3 = [b]_3 = [0]_3$.
Then we have
$$[c^2]_3 = [a^2]_3 + [b^2]_3 = [0]_3,$$
so c^2 is also a multiple of 3, which isn't PPT.
Next we consider $[a]_3 = [b]_3 = [1]_3$. Then we have
$$[c^2]_3 = [a^2]_3 + [b^2]_3 = [1]_3 + [1]_3 = [2]_3,$$
so $[c^2]_3 = [2]_3$, which is false due to our aforementioned lemma we can't generate a PPT.
Next consider $[a]_3 = [b]_3 = [2]_3$. Then we have
$$[c^2]_3 = [a^2]_3 + [b^2]_3 = [4]_3 + [4]_3 = [8]_3 = [2]_3,$$
like earlier it's not a PPT.
Finally, consider $[a]_3 = [1]_3$, $[b] = [2]_3$, provided without loss of generality. Then we have
$$[c^2]_3 = [a^2]_3 + [b^2]_3 = [1]_3 + [4]_3 = [5]_3 = [2]_3.$$
Hence like earlier it's not a PPT.

(b) We can guess that exactly one of the a, b, c is a multiple of 5.

First we prove the following Lemma.

Lemma. For any $c \in \mathbb{Z}_5$ we have $[c^2]_5 \neq [2]_5$ and $[c^2]_5 = [3]_5$.

Proof. We have the following $[1^2]_5 = [1]_5$, $[2^2]_5 = [4]_5$, $[3^2]_5 = [9]_5 = [4]_5$, $[4^2]_5 = [16]_5 = [1]_5$. ∎

We consider neither a and b aren't divisible by 5.
However
$$[1^2]_5 + [1^2]_5 = [2]_5,$$
$$[2^2]_5 + [2^2]_5 = [8]_5 = [3]_5,$$
$$[3^2]_5 + [3^2]_5 = [18]_5 = [3]_5,$$
$$[4^2]_5 + [4^2]_5 = [32]_5 = [2]_5,$$
$$[1^2]_5 + [2^2]_5 = [5]_5 = [0]_5,$$
$$[1^2]_5 + [3^2]_5 = [10]_5 = [0]_5,$$
$$[1^2]_5 + [4^2]_5 = [17]_5 = [2]_5,$$
$$[2^2]_5 + [3^2]_5 = [13]_5 = [3]_5,$$
$$[2^2]_5 + [4^2]_5 = [20]_5 = [0]_5,$$
$$[3^2]_5 + [4^2]_5 = [25]_5 = [0]_5.$$
Thus exactly one is divisible by 5.

2. Suppose $d \mid m$ and $d \mid n$. Then we have $m = dk$ and $n = dj$ for some k, j.
Thus
$$m + n = dk + dj = d(k + j), \text{ and}$$
$$m - n = dk - dj = d(k - j).$$
Hence $d \mid (m+n)$ and $d \mid (m-n)$. ∎

6. (a) Then we have:
$$(99, 20, 101)$$
and
$$(143, 24, 145)$$

(b) Given $c > 1000$ and $c = a + 2$ we have $a > 998$. Thus we get
$$a^2 + b^2 = c^2 = (a+2)^2 = a^2 + 4a + 4,$$
so $b^2 = 4a + 4$,
$(b/2)^2 = a + 1$, hence
$a = (b/2)^2 - 1$.
Thus if $b = 200$ then
$$a = (200/2)^2 - 1 = 100^2 - 1 = 9999.$$
Therefore $9999^2 + 200^2 = 100020001 = 10001^2$.

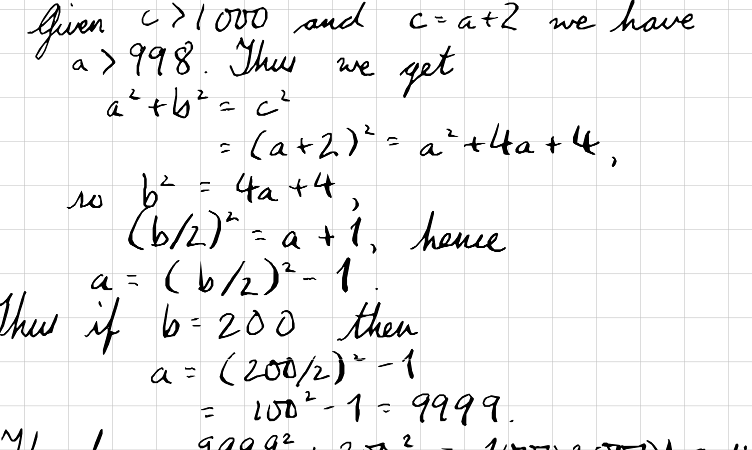
(c) Thus we have our PPT of
$$(a, b, c) = ((b/2)^2 - 1, b, a+2) = ((b/2)^2 - 1, b, (b/2)^2 + 1).$$

7. Note that

a b c	2c − 2a
3 4 5	$4 = 2^2$
5 12 13	$16 = 4^2$
7 24 25	$36 = 6^2$,

so is a squared even number.

Thus for all a, c, we have
$$2c - 2a = s^2 + t^2 - 2st = (s-t)^2,$$
hence since s, t are odd $s - t$ is even.

9. (a)

1 2 3 4 5 6 7
8 9 10 20 30 40
50

(b) The Plimpton 322 is a clay tablet showing the Pythagorean Triple since 1800 BC.

(c)

3.1 (a) If u and v has a common factor then we have $s = \gcd(u,v)$, so $k \mid u$ and $k \mid v$. Thus $u = km$ and $v = kn$ for some m, n. Thus

$$\begin{aligned}(a,b,c) &= (u^2-v^2,\ 2uv,\ u^2+v^2)\\ &= (k^2(m^2-n^2),\ k^2(2mn),\\ &\qquad k^2(m^2+n^2)).\end{aligned}$$

Thus it cannot be a PPT.

(b) Given $5 > 3 > 0$. Then we have

$$\begin{aligned}(a,b,c) &= (u^2-v^2,\ 2uv,\ u^2+v^2)\\ &= (5^2-3^2,\ 2(5)(3),\ 5^2+3^2)\\ &= (16,\ 30,\ 34),\end{aligned}$$

which is not a PPT since all are factors of 2.

(c) Given $10 \geq u > v \geq 1$. Then we have

See table

(d) To generate a PPT we require

i) $v<u$ or $u<v$,

ii) either u is odd and v is even, or vice versa,

iii) u and v has no common factors.

(e)

i) By contradiction, we consider $v = u$. Then we have

$$\begin{aligned}(a,b,c) &= (u^2-v^2,\ 2uv,\ u^2+v^2)\\ &= (0,\ 2u^2,\ 2u^2),\end{aligned}$$

which has a common factor of 2, so $v \neq u$. Hence $v<u$ or $u<v$.

ii) By contradiction, we consider both u, v either be even or odd. Then we consider two cases.

Case 1. u, v are both even. Then $u = 2m$, $v = 2n$ for some $m, n \in \mathbb{Z}$. Thus

$$\begin{aligned}(a,b,c) &= (u^2-v^2,\ 2uv,\ u^2+v^2)\\ &= ((2m)^2-(2n)^2,\ 2(2m)(2n),\ (2m)^2+(2n)^2)\\ &= (4(m^2-n^2),\ 8mn,\ 4(m^2+n^2)),\end{aligned}$$

which all have a factor of 4; similarly for odd we have

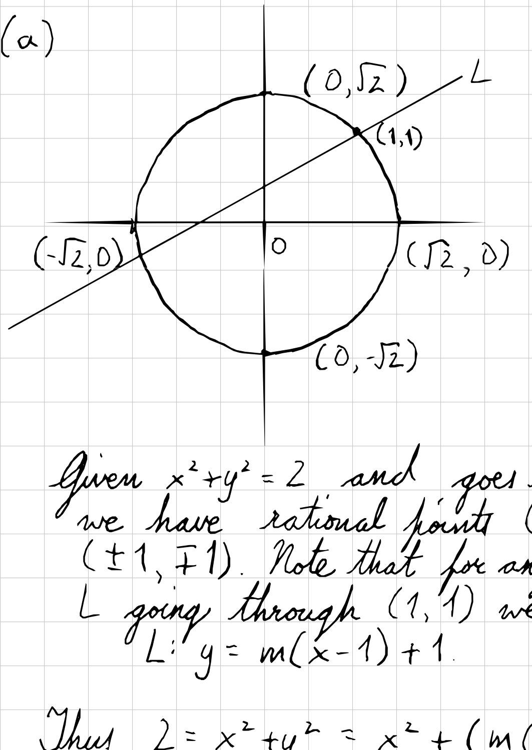
$$\begin{aligned}(a,b,c) &= ((2m+1)^2-(2n+1)^2,\\ &\qquad 2(2m+1)(2n+1),\\ &\qquad (2m+1)^2+(2n+1)^2)\\ &= (4m^2+4m+1-4n^2-4n-1,\\ &\qquad 2(4mn+2m+2n+1),\\ &\qquad 4m^2+4m+1+4n^2+4n+1)\\ &= (4(m^2+m-n^2-n),\\ &\qquad 2(4mn+2m+2n+1),\\ &\qquad 2(2m^2+2m+2n^2+2n+1))\end{aligned}$$

which all have a factor of 2. Therefore both cases aren't PPT, so either one of u, v can be even or odd.

iii) By definition of PPT. ∎

3.2

(a)



Given $x^2+y^2=2$ and goes through $(1,1)$, we have rational points $(\pm1, \pm1)$ and $(\pm1, \mp1)$. Note that for any rational of L going through $(1,1)$ we have

$L: y = m(x-1)+1$.

Thus

$$\begin{aligned}2 = x^2+y^2 &= x^2 + (m(x-1)+1)^2\\ &= x^2 + m^2(x-1)^2 + 2m(x-1)+1\\ &= x^2 + m^2(x^2-2x+1) + 2xm - 2m + 1\\ &= x^2 + x^2m^2 - 2xm^2 + m^2 + 2xm - 2m + 1,\end{aligned}$$

we have

$$\begin{aligned}0 &= x^2 + x^2m^2 - 2xm^2 + m^2 + 2xm - 2m - 1\\ &= (m^2+1)x^2 + (2m-2m^2)x + (m^2-2m-1).\end{aligned}$$

Note

$$\begin{aligned}x &= \frac{-(2m-2m^2) \pm \sqrt{(2m-2m^2)^2 - 4(m^2+1)(m^2-2m-1)}}{2(m^2+1)}\\ &= \frac{2m^2-2m \pm 2(m+1)}{2(m^2+1)},\end{aligned}$$

so

$$x = \frac{2m^2 \cancel{-2m} \cancel{+2m} + 2}{2(m^2+1)} = \frac{2(m^2+1)}{2(m^2+1)} = 1 \quad (\text{rejected})$$

or

$$x = \frac{2m^2-2m-2m-2}{2(m^2+1)} = \frac{2m^2-4m-2}{(m^2+1)} = \frac{m^2-2m-1}{m^2+1}.$$

Thus

$$\begin{aligned}y &= m(x-1)+1\\ &= m\left(\frac{m^2-2m-1}{m^2+1} - 1\right) + 1\\ &= m\left(\frac{\cancel{m^2}-2m-1\cancel{-m^2}-1}{m^2+1}\right)+1\\ &= \frac{m(-2m-2)+m^2+1}{m^2+1}\\ &= \frac{-2m^2-2m+m^2+1}{m^2+1} = \frac{-m^2-2m+1}{m^2+1}\end{aligned}$$

so every rational points

$$(x,y) = \left(\frac{m^2-2m-1}{m^2+1},\ \frac{-m^2-2m+1}{m^2+1}\right)$$

for $x^2+y^2=2$.

(b) To satisfy $x^2+y^2=3$, we require either x or y, or both to be irrational, and both can't be rational.

3.3 Given $x^2 - y^2 = 1$, it has two points that satisfies, which are $(\pm 1, 0)$.
Thus assuming a line L goes through point $(-1, 0)$.
Then $L: y = m(x+1)$.

Thus
$$\begin{aligned} 1 &= x^2 - y^2 \\ &= x^2 - (m(x+1))^2 \\ &= x^2 - m^2(x^2+2x+1) \\ &= x^2 - x^2m^2 - 2xm^2 - m^2 \\ &= (1-m^2)x^2 - 2xm^2 - m^2, \end{aligned}$$

so we have
$$0 = (1-m^2)x^2 - 2xm^2 - m^2 - 1,$$

so
$$\begin{aligned} x &= \frac{2m^2 \pm \sqrt{(-2m^2)^2 - 4(1-m^2)(-m^2-1)}}{2(1-m^2)} \\ &= \frac{2m^2 \pm 2}{2(1-m^2)}, \end{aligned}$$

so $x = \dfrac{1+m^2}{1-m^2}$ or $x = \dfrac{m^2-1}{-(m^2-1)} = -1$ (rejected).

Thus
$$\begin{aligned} y &= m(x+1) \\ &= m\left(\frac{1+m^2}{1-m^2} + 1\right) \\ &= m\left(\frac{1\cancel{+m^2}+1\cancel{-m^2}}{1-m^2}\right) \\ &= \frac{2m}{1-m^2}, \end{aligned}$$

so all rational points for $x^2 - y^2 = 1$ is
$$(x, y) = \left(\frac{1+m^2}{1-m^2}, \frac{2m}{1-m^2}\right).$$

3.4 Given $y^2 = x^3 + 8$ with points $(1, -3)$ and $(-7/4, 13/8)$. Then we consider the line passing through those points with $L: y = mx + c$.
Hence
$$m = \frac{-3 - 13/8}{1 - (-7/4)} = \frac{-37/8}{11/4} = \frac{-37}{22}.$$

Thus we have $-3 = \dfrac{-37}{22} + c$, so

$$y = \frac{-37}{22}x - \frac{29}{22}.$$ Hence we have

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

$$(-37x - 29)^2 = 484x^3 + 3872,$$

$$1369x^2 + 2146x + 841 = 484x^3 + 3872,$$

$$484x^3 - 1369x^2 - 2146x + 3031 = 0 \quad (1)$$

Note that $x = 1$ and $x = -7/4$ satisfies (1),
so $(x-1)(x+7/4) = x^2 + 3x/4 - 7/4$,
hence

$$\begin{array}{r} 484x - 1732 \\ x^2 + 3x/4 - 7/4 \,\big)\, 484x^3 - 1369x^2 - 2146x + 3031 \\ -\; 484x^3 + 363x^2 - 847x \\ -1732x^2 - 1299 + 3031 \\ -\; -1732x^2 - 1299 - 3031 \\ \hline 0 \end{array}$$

Hence we have
$$(484x - 1732)(x-1)(x+7/4) = 0,$$

so $x = 433/121$, hence

$$y = \left(\frac{-37}{22}\right)\left(\frac{433}{121}\right) - \frac{29}{22}$$

$=$, so our third point

is $(433/121, -9765/1331) =$

$(433/11^2, -9765/11^3)$.

It's rational due to having a polynomial of degree 1 as its solution for (1) without remainders.

Exercise 4.2

(a) Given $(a,b,c) = (xz, xy, z^2)$

$$a^3 + b^3 = c^2,$$
$$(xz)^3 + (yz)^3 = (z^2)^2,$$
$$x^3z^3 + y^3z^3 = z^4,$$
$$(x^3+y^3)z^3 = z^4,$$
$$x^3+y^3 = z.$$

Thus we have $x=2$, $y=1$, we have $2^3+1^3=9$, so $z=9$. Thus

$$a^3+b^3=c^2,$$
$$2^3\cdot 9^3 + 1^3\cdot 9^3 = 5832+729 = 6561 = 81^2,$$

so $(a,b,c) = (2,1,81)$.

Next we have $x=2$, $y=2$, we have $2^3+2^3=16$, so $z=16$. Thus

$$a^3+b^3=c^2,$$
$$2^3\cdot 16^3 + 2^3\cdot 16^3 = 2\cdot 32768 = 65536 = 256^2,$$

so $(a,b,c) = (32,32,256)$

Finally, we have $x=3$, $y=1$, we have $3^3+1^3=28$, so $z=28$. Thus

$$a^3+b^3=c^2,$$
$$3^3\cdot 28^3 + 1^3\cdot 28^3 = 592704 + 21952$$
$$= 614656 = 784^2,$$

so $(a,b,c) = (84,28,784)$.

(b) Consider $(a,b,c) = (n^2A, n^2B, n^3C)$. Then we have

$$(n^2A)^3 + (n^2B)^3 = (n^3C)^2,$$
$$n^6(A^3+B^3) = n^6C^2,$$

assuming $n \geq 2$ we have

$$A^3+B^3 = C^2.$$

(c) (i) We have $(2,1,81)$ to be our primitive.

(ii) We have $(32,32,256) = (2^5, 2^5, 2^8)$, so

$$(2^5)^3 + (2^5)^3 = (2^8)^2,$$
$$2^{15} + 2^{15} = 2^{16},$$
$$2^{12}(2^3+2^3) = 2^{12}\cdot 2^4,$$
$$2^3+2^3 = 4^2.$$

Thus its primitive solution is $(2,2,4)$

(iii) We have $(84,28,784) = (2^2\cdot 7\cdot 3, 2^2\cdot 7, 2^4\cdot 7^2)$, so

$$(2^2\cdot 7\cdot 3)^3 + (2^2\cdot 7)^3 = (2^4\cdot 7^2)^2,$$
$$2^6\cdot 7^3\cdot 3^3 + 2^6\cdot 7^3 = 2^8\cdot 7^4,$$
$$(7\cdot 3)^3 + 7^3 = 2^2\cdot 7^4$$
$$(7\cdot 3)^3 + 7^3 = (2\cdot 7^2)^2.$$

Thus $(21, 7, 98)$ is our primitive solution.

(d) Since $a=b$, we have

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

Thus c is even, so $c = 2k$ and

$$2a^3 = (2k)^2 \text{ for some } k,$$
$$= 4k^2,$$
$$a^3 = 2k^2,$$

so a is also even. Hence $a = 2j$, so

$$(2j)^3 = 2k^2 \text{ for some } j,$$
$$8j^3 = 2k^2,$$
$$4j^3 = k^2,$$

so k is also even. Thus $k = 2h$

$$4j^3 = (2h)^2, \text{ for some } h$$
$$4j^3 = 2^2h^2$$
$$j^3 = h^2.$$

Thus it follows that via our prime factoring theorem,

$$j = p_1^{t_1}p_2^{t_2}\cdots p_m^{t_m},$$
$$h = p_1^{s_1}p_2^{s_2}\cdots p_n^{s_n}.$$

Thus we have

$$j^3 = h^2 = p_1^{3t_1}p_2^{3t_2}\cdots p_m^{3t_m} = p_1^{2s_1}p_2^{2s_2}\cdots p_n^{2s_n},$$

so $p_i^{3t_i} = p_i^{2s_i}$, hence $3t_i = 2s_i$, which means $j^3 = h^2 = p_1^{6u_1}p_2^{6u_2}\cdots p_n^{6u_n} = z^6$. Thus $z^2 = j$ and $z^3 = h$.

Therefore since $a = b = 2j = 2z^2$ and $c^2 = 2a^3 = 2(2z^2)^3 = 16z^6$ so $c = 4z^4$

$$(a,b,c) = (a,a,c)$$
$$= (2z^2, 2z^2, 4z^4) = (z^2\cdot 2, z^2\cdot 2, z^3\cdot 4z)$$

if $z \neq 1$ then it's not primitive, otherwise we have $(2,2,4)$. ∎

(e) Using (a) consider $x=6$, $y=2$. Then

$$z = 6^3+2^3 = 216+8 = 224.$$

Thus $a = 6\cdot 224 = 1344$, $b = 2\cdot 224 = 448$, so $c = 224^2$. Thus since $a > 1000$,

$$a^3+b^3 = 224^4.$$

1. (a) $\gcd(12345, 67890) =$
$\gcd(67890, 12345)$, so
$67890 = 5 \cdot 12345 + 6165$,
$12345 = 2 \cdot 6165 + 15$,
$6165 = 441 \cdot 15 + 0$,
so $\gcd(12345, 67890) = 15$.

(b) $\gcd(54321, 9876)$, so
$54321 = 5 \cdot 9876 + 4941$,
$9876 = 1 \cdot 4941 + 4935$,
$4941 = 1 \cdot 4935 + 6$,
$4935 = 822 \cdot 6 + 3$,
$6 = 3 \cdot 2 + 0$,
so $\gcd(54321, 9876) = 3$.

2. We write in lisp

```
(define (gcd a b)
  (if (= b 0)
      a
      (gcd b (remainder a b))))
```

3. Let $b = r_0, r_1, r_2, \ldots$ Then using the Euclidean algorithm
$r_i = q_{i+2} r_{i+1} + r_{i+2}$ for every $i = 0, 1, 2$.
Then we have
$$r_i > r_{i+1} > r_{i+2}.$$
Hence since $q_{i+2} \geq 1$, we have
$$q_{i+2} r_{i+1} \geq r_{i+1} > r_{i+2},$$
$$q_{i+2} r_{i+1} + r_{i+2} \geq r_{i+1} + r_{i+2} > 2 r_{i+2},$$
$$r_i > 2 r_{i+2},$$
so
$$r_{i+2} < r_i/2.$$
Thus
$$r_i/2 > r_{i+2},$$
$$r_{i+2} > r_{i+3} > r_{i+4},$$
so since $q_{i+4} \geq 1$, we have
$$q_{i+4} r_{i+2} \geq r_{i+3} > r_{i+4},$$
$$q_{i+4} r_{i+2} + r_{i+4} \geq r_{i+3} + r_{i+4} > 2 r_{i+4},$$
$$r_{i+2} > 2 r_{i+4},$$
$$r_{i+2}/2 > r_{i+4},$$
so we have
$$r_i/4 > r_{i+2}/2 > r_{i+4},$$

so we have
$$r_i/2^k > r_{i+2^k} \quad \text{for } k = 1, 2, 3, \ldots$$
Thus it follows if
$$1 > r_0/2^k > r_{2^k},$$
we have $r_{2^k} = 0$.
Thus $2^k > r_0 > 0$,
so $2^k > r_0$,
hence $\log_2(2^k) > \log_2(r_0)$,
$k > \log_2(r_0)$,
$k > \log_2(b)$,
$k > \log(b)/\log(2)$,
hence we have $\log(b) =$ number of digits of b,
so $k \log(2)$ steps $>$ no. of digits of b.

We find x,y such that

$$22x + 60y = \gcd(60,22).$$

Note that

$$60 = 22\cdot 2 + 16$$
$$22 = 16\cdot 1 + 6$$
$$16 = 6\cdot 2 + 4$$
$$6 = 4\cdot 1 + 2$$
$$4 = 2\cdot 2 + 0,$$

so $\gcd(60,22) = 2$.

Thus we let $a = 60$, $b = 22$. Then for

$$\gcd(60,22) = 22x + 60y$$

we have

$a = b\cdot 2 + 16$	$16 = a - b\cdot 2 = a - 2b$
$b = 16\cdot 1 + 6$	$6 = b - 16\cdot 1 = b - (a-2b) = -a + 3b$
$16 = 6\cdot 2 + 4$	$4 = 16 - 6\cdot 2 = (a-2b) - (-a+3b)\cdot 2 = a - 2b + 2a - 6b = 3a - 8b$
$6 = 4\cdot 1 + 2$	$2 = 6 - 4\cdot 1 = (-a+3b) - (3a-8b)\cdot 1 = -a + 3b - 3a + 8b = -4a + 11b$
$4 = 2\cdot 2 + 0$	

Thus since $a = 60$, $b = 22$, we have

$$\gcd(60,22) = 60(-4) + 22(11).$$