# P. Set 12 Solutions

(1) By Fermat's little Theorem, $g^{p-1} \equiv 1 \bmod p$. Therefore, if $x = (p-1)q + r$, then

$$g^x = g^{(p-1)\cdot q + r}$$
$$= (g^{p-1})^q \cdot g^r$$
$$\equiv g^r \bmod p.$$

In other words, $g^x \equiv g^{x \% (p-1)} \bmod p$, where $x \% (p-1)$ denotes the remainder when $x$ is divided by $(p-1)$.

Since $g$ is a primitive root, the numbers $g^0, g^1, \cdots, g^{p-2}$ are all distinct modulo $p$. ~~So we know that if r~~
Therefore:

$\underline{g^x \equiv g^y \bmod p}$ is true if and only if $g^{x\%(p-1)} \equiv g^{y\%(p-1)}$,

which is true if and only if $x\%(p-1) = y\%(p-1)$,
(since $x\%(p-1)$ & $y\%(p-1)$ lie in $\{0, 1, \cdots, p-2\}$),

which is true if and only if $\underline{x \equiv y \bmod (p-1)}$.

(2) Let $x, y$ be such that $18^x \equiv 38 \bmod 101$ and $18^y \equiv 69 \bmod 101$. Then we know:

$$(18^x)^2 \cdot 18^y \equiv 18^{91} \bmod 101$$
$$\Leftrightarrow \quad 18^{2x+y} \equiv 18^{91} \bmod 101$$
$$\Leftrightarrow \quad \underline{2x + y \equiv 91 \quad \bmod 100} \qquad (1)$$

(by problem 1, since 18 is a prim. root).

By similar logic, $\underline{x + 2y \equiv 13 \bmod 100}$. $\qquad (2)$

Therefore:

$$y \equiv 91 - 2x \bmod 100 \qquad \text{(from (1))} \qquad (3)$$

$$\Rightarrow \quad x + 2(91-2x) \equiv 13 \bmod 100 \qquad \text{(from (2))}$$

$$\Rightarrow \quad -3x + 182 \equiv 13 \bmod 100$$

$$\Rightarrow \quad 69 \equiv 3x \bmod 100$$

$$\Rightarrow \quad \frac{69}{3} \equiv x \bmod 100 \qquad (\text{since } \gcd(3,100)=1)$$

so $\boxed{x \equiv 23 \bmod 100}$

Thus using (3),

$$y \equiv 91 - 2\cdot 23 \bmod 100$$

$$\boxed{y \equiv 45 \bmod 100}.$$

Therefore (modulo 100), $x$ must be 23 & $y$ must be 45.

③ a) $4370 = 2\cdot 5\cdot 437$
$= 2\cdot 5\cdot 19\cdot 23$

since $23 \equiv 3 \bmod 4$ and appears once in the prime factorization, 4370 is $\boxed{\text{not a sum of two squares.}}$

b) $1885 = 5\cdot 377$
$= 5\cdot 13\cdot 29.$

All three of these primes are SOTS.

$$5 = 2^2 + 1^2$$
$$13 = 3^2 + 2^2$$
$$29 = 5^2 + 2^2$$

We can combine as follows:

$$5\cdot 13 = (2\cdot 3 + 1\cdot 2)^2 + (2\cdot 2 - 1\cdot 3)^2$$
$$= 8^2 + 1^2$$

$$(5\cdot 13)\cdot 29 = (8\cdot 5 + 1\cdot 2)^2 + (8\cdot 2 - 5\cdot 1)^2$$
$$= \boxed{42^2 + 11^2}$$

There are three other possible answers: (you only needed to give one).

$$5\cdot 13 = (2\cdot 3 - 1\cdot 2)^2 + (2\cdot 2 + 1\cdot 3)^2$$
$$= 4^2 + 7^2$$
$$(5\cdot 13)\cdot 29 = (4\cdot 5 + 7\cdot 2)^2 + (4\cdot 2 - 5\cdot 7)^2$$
$$= 34^2 + (-27)^2$$
$$= \boxed{34^2 + 27^2}$$

$$5\cdot 13 = (2\cdot 3 - 1\cdot 2)^2 + (2\cdot 2 + 1\cdot 3)^2$$
$$= 4^2 + 7^2$$
$$(5\cdot 13)\cdot 29 = (4\cdot 5 - 7\cdot 2)^2 + (4\cdot 2 + 5\cdot 7)^2$$
$$= 6^2 + 43^2$$
$$\boxed{6^2 + 43^2}$$

$$5\cdot 13 = 8^2 + 1^2$$
(as before)

and

$$(5\cdot 13)\cdot 29 = (8\cdot 5 - 1\cdot 2)^2 + (8\cdot 2 + 5\cdot 1)^2$$
$$= \boxed{38^2 + 21^2}$$

c) $1189 = 29\cdot 41$. Both primes are $1 \bmod 4$, so they are SOTS.

$$29 = 5^2 + 2^2$$
$$41 = 5^2 + 4^2$$

$$\Rightarrow 29\cdot 41 = (5\cdot 5 + 2\cdot 4)^2 + (5\cdot 4 - 2\cdot 5)^2$$
$$= \boxed{33^2 + 10^2}$$

The other possible solution is

$$29\cdot 41 = (5\cdot 5 - 2\cdot 4)^2 + (5\cdot 4 + 2\cdot 5)^2$$
$$= \boxed{17^2 + 30^2}$$

d) $3185 = 5 \cdot 637$

$= 5 \cdot 7^2 \cdot 13.$

5 & 13 are 1 mod 4, and 7 occurs an even number of times.
so 3185 is SOTS.

$$5 = 2^2 + 1^2$$
$$13 = 2^2 + 3^2$$

$$\Rightarrow 5 \cdot 13 = (2 \cdot 2 + 1 \cdot 3)^2 + (2 \cdot 3 - 1 \cdot 2)^2 = 7^2 + 4^2$$

$$\left(\text{or} \quad = (2 \cdot 2 - 1 \cdot 3) + (2 \cdot 3 + 1 \cdot 2)^2 = 8^2 + 1^2.\right)$$

The factor of 7 can be introduced only by multiplying both terms to be squared by 7.

$$(5 \cdot 13) \cdot 7^2 = (7 \cdot 7)^2 + (4 \cdot 7)^2$$
$$= \boxed{49^2 + 28^2}$$

The other possible solution is $(8 \cdot 7)^2 + (1 \cdot 7)^2$

$$= \boxed{56^2 + 7^2}$$

4 $\quad 557^2 + 55^2 = 26 \cdot 12049$

$557 \equiv 11 \bmod 26$ and $55 \equiv 3 \bmod 26$, so
~~descent~~ reduce to:

$$\left(\frac{557 \cdot 11 + 55 \cdot 3}{26}\right)^2 + \left(\frac{557 \cdot 3 - 55 \cdot 11}{26}\right)^2 = \frac{11^2 + 3^2}{26} \cdot 12049$$

$$\left(\frac{6292}{26}\right)^2 + \left(\frac{1066}{26}\right)^2 = \frac{130}{26} \cdot 12049$$

$$\underline{242^2 + 41^2 = 5 \cdot 12049}$$

descend again:

$242 \equiv 2 \bmod 5 \qquad 41 \equiv 1 \bmod 5$

so go to

$$\left(\frac{242\cdot 2 + 41\cdot 1}{5}\right)^2 + \left(\frac{242\cdot 1 - 41\cdot 2}{5}\right)^2 = \frac{2^2+1^2}{5}\cdot 12049$$

$$\left(\frac{525}{5}\right)^2 + \left(\frac{160}{5}\right)^2 = 12049$$

$$\cancel{105^2 + 26^2}$$

$$\boxed{105^2 + 32^2 = 12049}$$