Solutions to HW1

In #1,2, I will list Pythagorean triples as (a, b, c) in increasing order $(a, b < c)$, referring to c as the *hypotenuse* and a, b as the *legs*. Recall that in a *primitive* Pythagorean triple, the hypotenuse must be congruent to 1 mod 4.

1. There are eight different Pythagorean triples containing 40:

$$(24, 32, 40),\ (9, 40, 41)^*,\ (30, 40, 50),\ (40, 96, 104),\ (42, 40, 58),$$
$$(75, 40, 85),\ (198, 40, 202),\ (399, 40, 401)^*.$$

   Of these, only two (marked with asterisks) are primitive. The only Pythagorean triple having 40 as its hypotenuse is $(24, 32, 40)$. Recall that every primitive Pythagorean triple has hypotenuse congruent to 1 mod 4; and the only divisors of 40 congruent to 1 mod 4 are 1 and 5. The primitive Pythagorean triple $(3, 4, 5)$, scaled by a factor of 8, gives the first solution on our list.

   For the Pythagorean triples having a leg equal to 40, it is possible to consider all primitive Pythagorean triples having a leg which divides 40; but we believe this approach is longer due to the complicated nature of the cases under consideration. So we have opted instead to argue more directly from the definition. Every Pythagorean triple $(40, b, c)$ having c as its hypotenuse, satisfies $40^2 = c^2 - b^2 = (c+b)(c-b)$ where both b and c are even (since $c+b$ and $c-b$ have the same parity, and they cannot both be odd). Setting $c+b = 2s$ and $c-b = 2t$, we have $c = s+t$ and $b = s-t$ where $40^2 = 4st$ and $st = 400$. Since $1 \leqslant t < s$, we have $t < \sqrt{400} = 20$. There are exactly seven divisors of 400 less than 20, namely $t \in \{1, 2, 4, 5, 8, 10, 16\}$. This gives the last seven Pythagorean triples in our list above.

2. Every positive integer except 1 and 2 is contained in a Pythagorean triple. First suppose a, b, c are positive integers with $a^2 + b^2 = c^2$, so we may assume $a \leqslant b < c$. If $a = b$ then $2a^2 = c^2$ which is impossible; so $b > a$ and $b \geqslant 2$. Now $a^2 = c^2 - b^2 \geqslant (b+1)^2 - b^2 = 2b+1 \geqslant 5$ so $a > 2$ and all members of the Pythagorean triple are at least 3.

   Conversely, every integer $m \geqslant 3$ is contained in some Pythagorean triple. If $m = 2k$ $(k \geqslant 2)$ then m is contained in the triple $(k^2-1,\ 2k,\ k^2+1)$; and if $m = 2k+1$ $(k \geqslant 1)$ then m is contained in the triple $(2k+1,\ 2k^2+2k,\ 2k^2+2k+1)$.

3.

631	101	
1	0	631
0	1	101
1	−6	25
−4	25	(1)
101	−631	0

(a) This gives the simplest integer solution of

$$\gcd(631, 101) = 1 = 631r + 101s,$$

namely, $(r, s) = (-4, 25)$. The *last* row gives the simplest integer solution of $631r + 101s = 0$. Putting this together gives *all* integer solutions of

$$631r + 101s = 1,$$

namely, $(r, s) = (-4+101k,\ 25-631k)$.

(b) The inverse of 631 mod 101 is 97 (or -4).

Note the difference between #3 and #4: in #3 we work in $\mathbb{Z}$, whereas in #4, we work in $\mathbb{F}_{101}$. In #3 we have *congruences* in $\mathbb{Z}$, such as $97 \cdot 631 \equiv 1 \mod 101$. In #4, we have *equations* in $\mathbb{F}_{101}$, such as $6603 = 38$.

4. In $\mathbb{F}_{101}$, $\begin{bmatrix} 28 & 71 \\ 91 & 47 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 38 \\ 22 \end{bmatrix}$ so $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 28 & 71 \\ 91 & 47 \end{bmatrix}^{-1}\begin{bmatrix} 38 \\ 22 \end{bmatrix}$
$= -\frac{1}{5145}\begin{bmatrix} 47 & -71 \\ -91 & 28 \end{bmatrix}\begin{bmatrix} 38 \\ 22 \end{bmatrix} = 17\begin{bmatrix} 22 \\ 87 \end{bmatrix} = \begin{bmatrix} 71 \\ 65 \end{bmatrix}$. We used $-\frac{1}{5145} = \frac{1}{6} = 17$, computed (on the right) by Euclid's Algorithm.
Check: $28 \cdot 71 + 71 \cdot 65 = 6603 = 38$; $91 \cdot 71 + 47 \cdot 65 = 9516 = 22$.

101	6	
1	0	101
0	1	6
1	−16	5
−1	17	(1)

5. (a) $89 = 8^2 + 5^2$ (b) $137 = 11^2 + 4^2$

(c) We have $89 = |\alpha|^2$ and $137 = |\beta|^2$ where $\alpha = 8 + 5i$ and $\beta = 11 + 4i$, so $12193 = 89 \cdot 137 = |\alpha\beta|^2 = |\overline{\alpha}\beta|^2$. Here $\alpha\beta = 68 + 87i$ and $\overline{\alpha}\beta = 108 - 23i$, so $12193 = 68^2 + 87^2 = 108^2 + 23^2$.

6. (a) $43 = 6^2 + 7 \cdot 1^2$ (b) $79 = 4^2 + 7 \cdot 3^2$

(c) Let $\theta = \sqrt{-7}$. We have $43 = |\alpha|^2$ and $79 = |\beta|^2$ where $\alpha = 6 + \theta$ and $\beta = 4 + 3\theta$, so $3397 = 43 \cdot 79 = |\alpha\beta|^2 = |\overline{\alpha}\beta|^2$. Here $\alpha\beta = 3 + 22\theta$ and $\overline{\alpha}\beta = 45 + 14\theta$, so $3397 = 3^2 + 7 \cdot 22^2 = 45^2 + 7 \cdot 14^2$.