
# Solutions to the Test

April, 2025

1. $61n = (5a-6b)^2 + (6a+5b)^2$. To obtain this, use $n = |z|^2$ and $61 = |w|^2$ where $z = a+bi$, $w = 5+6i$; so $61n = |zw|^2$ where $zw = (5a-6b) + (6a+5b)i$.

---

2. (a)

| 402 | 147 | |
|---|---|---|
| 1 | 0 | 402 |
| 0 | 1 | 147 |
| 1 | −2 | 108 |
| −1 | 3 | 39 |
| 3 | −8 | 30 |
| −4 | 11 | 9 |
| 15 | −41 | 3 |
| −49 | 134 | 0 |

From the second-last row,
$\gcd(402, 147) = 3 = 407r + 147s$ where $(r, s) = (15, -41)$ (the *simplest* solution for $(r, s)$).

(b) All solutions are given by $(r, s) = (15 - 49t, -41+134t)$ for $t \in \mathbb{Z}$. In particular, $t = -2, -1, \ldots, 2$ gives the five simplest solutions
$(113, -309)$, $(64, -175)$, $(15, -41)$, $(-34, 93)$, $(-83, 227)$.

(c) By (a), the simplest way to pay \$3 is to give 15 grots, and get back 41 klins in change.

---

3. *Proof.* Let $d = \gcd(a, b)$. By Euclid's **algorithm**, we have $d = xa+yb$ for **some** $x, y$. Now we prove the statement of the Theorem, beginning with the forward direction.

Assuming $g$ is **divisible** by $d$, then $g = cd$ for **some** integer $c$. In this case, $g = (cx)a + (cy)b$, as **required**.

Conversely, **suppose** $g = ra + sb$ for **some** $r, s \in \mathbb{Z}$. Since $d$ divides $a$ and $b$, it also **divides** $ra + sb = g$. This completes the **proof**.

---

4. (a) Since $4^{p-1} \not\equiv 1 \mod p$, we conclude that $p$ is not prime, i.e. $p$ is composite.

(b) No, from $4^{r-1} \equiv 1 \mod r$, we have some basis for suspecting that $r$ may be prime; but this test is inconclusive for proving such a fact.

---

5. By HW1 #2, every integer $\geqslant 3$ is contained in a Pythagorean triple. So let $p$ be any odd integer $\geqslant 3$. (We don't really require that $p$ is prime.) Then $p$ is contained in the Pythagorean triple $\big(p,\ \frac{1}{2}(p^2-1),\ \frac{1}{2}(p^2+1)\big)$. This is found by first seeing that the only hope for a Pythagorean triple containing $p$ is a primitive triple of the form $(m^2-n^2,\ 2mn, m^2+n^2)$ with $m^2-n^2 = p$. This requires $m+n = p$, $m-n = 1$, which can be uniquely solved for $m$ and $n$.

---

6.

| (a) | (b) | (c) | (d) | (e) | (f) | (g) | (h) | (i) | (j) |
|---|---|---|---|---|---|---|---|---|---|
| $T$ | $F$ | $T$ | $T$ | $T$ | $F$ | $F$ | $F$ | $F$ | $T$ |

Although you are not expected to explain your answers to True/False questions, the following remarks may help to understand the solution key:

(a) Fundamental Theorem of Arithmetic

(b) If $a^2 + b^2 = 1200^2$ then $a, b \leqslant 1200$, for which only finitely many positive integers $a, b$ are permissible. If $a^2 + 1200^2 = c^2$ then $c = \sqrt{1200^2-a^2} \leqslant 1200$; again, only finitely many integer solutions are possible.

(c) Euclid's proof is well known (and was presented in class).

(d) This follows from the more general fact that Pell's equation always has infinitely many solutions. In fact, the ring $R = \mathbb{Z}[\sqrt{17}]$ has norm map $N : R \to \mathbb{Z}$ satisfying $N(\alpha\beta) = N(\alpha)N(\beta)$, where $N(a+b\sqrt{17}) = a^2 - 17b^2$. Since $N(u) = -1$ where $u = 4+\sqrt{17}$ (a unit), $R$ has infinitely many elements $\pm u^{2k}$ for $k \in \mathbb{Z}$ of norm 1. For $k = 0, \pm1, \pm2, \ldots$, the simplest solutions are $(\pm1, 0)$, $(\pm33, \pm8)$, $(\pm2177, \pm528)$, ....

(e) This special case of Fermat's Last Theorem has been known for over three hundred years.

(f) No such algorithm exists, as mentioned in class. Not only is no such algorithm known; but in fact no such algorithm can possibly exist. Look up 'MDRP Theorem' or 'Hilbert's Tenth Problem' for further details.

(g) Euclid's algorithm computes $\gcd(m, n)$ very efficiently.

(h) Current methods (hardware and software) do not allow us to factor typical integers of more than about 250 decimal digits. There is no realistic expectation for this situation to change in the near future (and in many ways this is a good thing).

(i) Since 24 and 100 are not relatively prime, $\phi(2400) > \phi(24)\phi(100)$. In fact, $\phi(24) = 8$, $\phi(100) = 40$, $\phi(2400) = 640$.

(j) This follows from the Chinese Remainder Theorem, since $2^6$ and $5^6$ are relatively prime. (The solution, found by the method demonstrated in class, is $x = 582042$.)