Solutions to Practice Test Problems

1. (a) $2025 = 3^4 \cdot 5^2$ has 30 divisors $\pm 3^i 5^j$ for $i \in \{0,1,2,3,4\}$, $j \in \{0,1,2\}$. Explicitly, these divisors are $\pm 1, \pm 3, \pm 5, \pm 9, \pm 15, \pm 25, \pm 27, \pm 45, \pm 75, \pm 81, \pm 135, \pm 243, \pm 405, \pm 675, \pm 2025$.

   (b) $\phi(2025) = 3^3(3-1)5(5-1) = 1080$.

   (c) $\gcd(81, n) = 81 = 1 \cdot 81 + 0 \cdot 2025$. Oops, I didn't really intend for this to be so trivial ... I hope you can also manage to do a more elaborate example. Since 81 divides 2025, this is a one-line computation.

   (d) No, the solution in (c) is far from unique; all integer solutions of $81r + 2025s = 81$ are given by $(r, s) = (1 + 25k, -k)$ where $k \in \mathbb{Z}$.

---

2. We claim that the solutions are the integers of the form $x = 143r + 71$ for $r \in \mathbb{Z}$. It is straight-forward to prove that these integers solve the indicated congruences; so it remains only to prove the converse.

   By Euclid's algorithm (or by inspection), we find $6 \cdot 11 - 5 \cdot 13 = 1$. Let x be any solution of the two given congruences, so that $x = 11k + 5$ for some $k \in \mathbb{Z}$. Multiplying both sides by 6 gives $k \equiv 6x - 30 \equiv 36 - 30 \equiv 6 \mod 13$, so $k = 13r + 6$ for some $r \in \mathbb{Z}$. This gives $x = 11(13r + 6) + 5 = 143r + 71$ as claimed.

---

3. Given $n = pq$ and $\phi(n) = (p-1)(q-1)$, we find p and q as the roots of the quadratic equation

$$(x - p)(x - q) = x^2 - (n - \phi(n) + 1)x + n = 0.$$

   The roots are

$$p, q = \tfrac{1}{2}\left[n - \phi(n) + 1 \pm \sqrt{(n - \phi(n) + 1)^2 - 4n}\right].$$

   The point here is that if n, p, q are several hundred digits in length, then factorization of n is not possible without additional information. However, being given the explicit value of $\phi(n) = (p-1)(q-1)$, in addition to $n = pq$, allows us to easily solve for p and q. This simple fact will be important later in the semester when we study RSA cryptography.

4. No. Every integer triple of the form $(m^2-n^2, 2mn, m^2+n^2)$ is Pythagorean, but not conversely unless the triple is primitive. For example, the Pythagorean triple $(9, 12, 15)$ does not have the indicated form. To see this, note that the largest member of the indicated triple satisfies $m^2+n^2 \not\equiv 3 \mod 4$ whereas $15 \equiv 3 \mod 4$.

---

5. By the extended Euclidean Algorithm, find integers a, b such that $am + k(p-1) = 1$. Let $g \equiv r^a \mod p$. By Fermat's Little Theorem,

$$g^m \equiv (r^a)^m \equiv r^{am} 1^k \equiv r^{am}(r^{p-1})^k \equiv r^{am+k(p-1)} = r^1 = r \mod p.$$

Here we are assuming that $\gcd(r, p) = 1$; if, however, r is divisible by p, then one may instead simply choose $g = 0$.

---

6. The nonzero elements of $\mathbb{F}_p$, except for 1 and -1, occur in pairs $\{a, a^{-1}\}$. So in the product

$$\prod_{0 \neq a \in \mathbb{F}_p} a\,,$$

all factors cancel (in pairs) except for the factors 1 and -1, leaving a value of -1 as the final value of the product. (Of course when $p = 2$ there is really only *one* such factor since $-1 = 1$ in this case; but our answer holds since the final product is once again $-1 = 1$.)

---

7. We have $n = z\overline{z}$ and $26 = w\overline{w}$ where $z, w \in \mathbb{Z}[i]$ are given by $z = a+bi$ and $w = 5+i$, so $26n = (zw)(\overline{zw}) = c^2 + d^2$ where $zw = c + di = (5a-b) + (a+5b)i$. An essentially different solution is given by $(c, d) = (5a+b,\ a-5b)$.

---

8. If a is relatively prime with $1105 = 5{\cdot}13{\cdot}17$, then by Fermat's Little Theorem

$$a^{1104} = (a^4)^{276} \equiv 1^{276} \equiv 1 \mod 5;$$
$$a^{1104} = (a^{12})^{92} \equiv 1^{92} \equiv 1 \mod 13; \text{ and}$$
$$a^{1104} = (a^{12})^{69} \equiv 1^{69} \equiv 1 \mod 17$$

so $a \equiv 1 \mod 1105$. (This last conclusion follows from the Chinese Remainder Theorem; but it is a more direct consequence of the fact that $a - 1$ is divisible by three primes 5, 13 and 17, so it is divisible by their product.) Indeed, after 561 (the smallest Carmichael number, featured in class, the next smallest Carmichael number is 1105.

9. We show that $n = 2\phi(n)$ iff $n \in \{2, 4, 8, 16, 32, \ldots\}$. Clearly all solutions have $n > 1$, so we may write $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ where $p_1 < p_2 < \cdots < p_k$ are the distinct prime divisors of n, with $k, e_1, \ldots, e_k \geqslant 1$. If $n = 2\phi(n) = 2\prod_{i=1}^{k}(p_i^{e_i} - p_i^{e_i-1})$, then we obtain $\prod_{i=1}^{k} p_i = 2\prod_{i=1}^{k}(p_i - 1)$. If p_k is odd, then the left side is divisible by the prime p_k, but the right side is not, a contradiction. So n has no odd prime divisors. This means $n = 2^e$ with $e \geqslant 1$, and $\phi(n) = 2^e - 2^{e-1} = 2^{e-1}$, so $n = 2\phi(n)$.

---

10. No, it is not possible for $f(n)$ to be prime for every positive integer n. Since $f(x)$ is nonconstant, it is either increasing or decreasing for all sufficiently large x. In the decreasing case, $f(x)$ is eventually negative for large x, and therefore not prime; so we may assume there is a positive integer n such that $f(x)$ is increasing for $x \geq n$. By assumption, $p = f(n)$ is prime. Also $f(n+p) \equiv f(n) \equiv p \equiv 0 \mod p$, i.e. $f(n+p)$ is divisible by p. Since $f(n+p)$ is also prime, we must have $f(n+p) = p$. This contradicts $f(n+p) > f(n)$.

    We remark that the polynomial $f(x) = x^2 - x + 41$ famously gives prime values $f(n)$ for $n = 0, 1, 2, \ldots, 40$; but then $f(41)$ is prime. This is *not* a fluke! It happens only because of a very special property of the number 41, and of the value -163 which is the discriminant of the polynomial $f(x)$. It is related to the amazing value

$$e^{\pi\sqrt{163}} = 262\,537\,412\,640\,768\,743.999\,999\,999\,999\,25\ldots$$

---

11. Yes. If p is composite, then there exists $a \in \{2, 3, \ldots, p-1\}$ dividing p; but then $\gcd(a^{p-1}, p) \geqslant a > 1$. (Note: Carmichael numbers are no exception to this fact. In order for n to be a Carmichael number, one only requires $a^{n-1} \equiv 1 \mod n$ for every *a relatively prime to n*.)

12.

a	b	c	d	e	f	g	h	i	j
F	*F*	*F*	*F*	*F*	*F*	*T*	*F*	*F*	*F*

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

(a) The equation $x^3 + y^3 = z^3$ has *no* solutions in positive integers. This special case of Fermat's Last Theorem was proved many decades before the full theorem was finally proved.

(b) Fermat's Little Theorem is used to verify that certain numbers are composite; but it is of no direct value in finding prime factors of integers.

(c) $N^2 - 1 = (N + 1)(N - 1)$ is prime only for $N = \pm 2$. There is no known polynomial in N (of degree at least 2, with integer coefficients) which is known to give infinitely many prime values. Even the simplest example, $N^2 + 1$, is not known to give infinitely many prime values (see Chapter 13).

(d) A counterexample is given by $4 \cdot 2 \cdot 5 - 1 = 3 \cdot 13$.

(e) This is the famous *conjecture* of Goldbach; see Chapter 13.

(f) Consider that 6 divides $4 \cdot 9 = 36$, but 6 divides neither 4 nor 9. (This shows that in the statement of Euclid's Lemma, the hypothesis that p is prime is essential.)

(g) This fact, which is easily proved using the Fundamental Theorem of Arithmetic, was used in our classification of primitive Pythagorean triples.

(h) The affirmative answer is a general fact about Pell's equation which was stated in our February 19 lecture. We remark that the solutions of $x^2 - 19y^2 = 1$ arise from $x + y\sqrt{19} = \pm(170 + 39\sqrt{19})^n$ where $n \in \mathbb{Z}$.

(i) The only prime p for which $p^2 + 1$ is prime, is $p = 2$. All larger values of the prime p yield an even value of $p^2 + 1 \geqslant 10$. See also comments on (c).

(j) A counterexample is given by $r = s = a = b = 1$. From the relation $ra + sb = d$, one can conlcude only that $\gcd(a, b)$ divides d, not that $\gcd(a, b) = d$.