Solution for PS5-1.

a. By repeated application of "Theorem 6" from the lecture notes,

$$\begin{aligned}\gcd(13631, 8213) &= \gcd(8213, 13631 \bmod 8213)\\ &= \gcd(5418, 8213 \bmod 5418)\\ &= \gcd(2795, 5418 \bmod 2795)\\ &= \gcd(2623, 2795 \bmod 2623)\\ &= \gcd(172, 2623 \bmod 172)\\ &= \gcd(43, 172 \bmod 43)\\ &= \gcd(43, 0) = 43\,.\end{aligned}$$

b. Using the Extended Euclidean Algorithm,

$$\begin{aligned}43 &= 1\cdot 43 + 0\cdot 0 && \text{Base case, } k_0 = 1;\ \ell_0 = 0\\ &= 0\cdot 172 + 1\cdot 43 && k_1 = \ell_1 = 0;\ \ell_1 = k_0 - \lfloor a_1/b_1\rfloor\cdot\ell_0 = 1 - \lfloor 172/43\rfloor\cdot 0\\ &= 1\cdot 2623 - 15\cdot 172 && k_2 = 1;\ \ell_2 = 0 - \lfloor 2623/172\rfloor\cdot 1\\ &= -15\cdot 2795 + 16\cdot 2623 && k_3 = -15;\ \ell_3 = 1 - \lfloor 2795/2623\rfloor\cdot(-15)\\ &= 16\cdot 5418 - 31\cdot 2795 && k_4 = 16;\ \ell_4 = -15 - \lfloor 5418/2795\rfloor\cdot 16\\ &= -31\cdot 8213 + 47\cdot 5418 && k_5 = -31;\ \ell_5 = 16 - \lfloor 8213/5418\rfloor\cdot -31\\ &= 47\cdot 13631 - 78\cdot 8213 && k_6 = 47;\ \ell_6 = -31 - \lfloor 13631/8213\rfloor\cdot 47\end{aligned}$$

we find $k = 47$, $\ell = -78$.

c. Consider $k = 47 - 8213/43 = -144$, and $\ell = -78 + 13631/43 = 239$.

Solution for PS5-2.

a. False. Take $a = 2$, $b = 6$, and $c = 3$.

b. True. This is because $d \mid c \iff d^n \mid c^n$. The reverse implication isn't straightforward, but can be proved using the Unique Factorization Theorem.

c. True. If $d = \gcd(b, c)$, then clearly ad is a common divisor of ab and ac. On the other hand, by LCT, $\exists\, k, \ell \in \mathbb{Z}$ such that $d = kb + \ell c$, so $ad = kab + \ell ac$, whence $\gcd(ab, ac) \mid ad$.

d. False. Take $a = 2$, $b = 4$.

e. True. If $ka + \ell b = 1$, then $\ell^2 b^2 = (1 - ka)^2 = k^2a^2 - 2ka + 1$. Therefore, $(2k - k^2a)a + \ell^2 b^2 = 1$.

f. True. The given condition implies $g := \gcd(a, b) \geq 3$. Clearly, $\gcd(a^2, b^2) \geq g \geq 3$. Had 2 been an IntLC of a^2 and b^2, we would have had $\gcd(a^2, b^2) \mid 2$.

Solution for PS5-3.

a. The code doesn't handle negative numbers correctly. Calling egcd(9, −6) returns (−3, 1, 2). However, by definition gcd(9, −6) = 3, not −3.

b.

```
def egcd(a, b):
    if b < 0:
        g, k, l = egcd(a, -b)
        return (g, k, -l)
    elif a < 0:
        g, k, l = egcd(-a, b)
```

```
        return (g, -k, l)
    elif b == 0:
        return (a, 1, 0)
    else:
        g, k, l = egcd(b, a % b)
        return (g, l, k - (a // b) * l)
```

Solution for PS5-4.

a. Assume that a good call egcd(a, b) is made, so that $0 \neq a \geq b \geq 0$. If it makes an immediate recursive call, $b \neq 0$. The new call is egcd(b, r), where $r = a \bmod b$. By definition of the "mod" operation, $r < b$. Therefore, $0 \neq b \geq r \geq 0$, i.e., the new call is good. Furthermore, the size of the new call is

$$b + r < b + b \leq b + a = s\,.$$

b. Consider the sequence of sizes of all recursive calls that result from an initial good call to egcd. By the above results, these recursive calls are all good, so the sizes are all natural numbers, and the sequence is decreasing. The sequence cannot be infinite (the sizes cannot decrease forever), so it eventually terminates, i.e., there is eventually a call to egcd that does not result in further recursion.

Solution for PS5-6.

a. Let $m = \text{lcm}(a, b)$. Being a positive multiple of a, m must equal ax for some $x \in \mathbb{N}^+$. Similarly, $m = by$ for some $y \in \mathbb{N}^+$. Now suppose that $\gcd(x, y) = z > 1$. Then x/z and y/z are both integers and so

$$\frac{ax}{z} = \frac{by}{z} = \frac{m}{z} < m$$

is a common multiple of a and b that is smaller than m, a contradiction.

b. By LCT, $\exists\, k, \ell \in \mathbb{Z}$ such that $1 = kx + \ell y$. Therefore, $a/y = kax/y + \ell ay/y = kb + \ell a$.

c. Since $d := \gcd(a, b)$ must divide every IntLC of a and b, in particular, $d \mid a/y$.

d. Since $a/y \in \mathbb{Z}$, it is obviously a divisor of a. Further, $b/(a/y) = by/a = x \in \mathbb{Z}$, so a/y divides b as well.

e. Since a/y is one particular common divisor of a and b, the *greatest* common divisor $d \geq a/y$. But we also showed that $d \mid a/y$. Therefore, $d = a/y$.

f. A simple calculation: $\gcd(a, b) \cdot \text{lcm}(a, b) = dm = (a/y)(by) = ab$.

Solution for PS5-7.

a. The only divisors of p are 1 and itself. Of these, only 1 is a divisor of b, since $0 < b < p$. Therefore, $\gcd(b, p) = 1$. By the Inverse Existence Theorem, b has an inverse modulo p.

b. Let $a = b^{-1}$. We claim that the function f_a is the inverse of f_b. Indeed,

$$f_a(f_b(x)) = f_a(bx \bmod p) = (a(bx \bmod p) \bmod p) = abx \bmod p = x\,,$$

so $f_a \circ f_b = \text{id}_{\mathbb{Z}_p}$. Similarly, $f_b \circ f_a = \text{id}_{\mathbb{Z}_p}$. By results from earlier in the course, f_b is a bijection.

Solution for PS5-8. The fact to be shown follows from its contrapositive, the statement that if n is not even, then n^2 is not even. This statement is precisely *PS3-1e*, the fact that the product of two odd numbers is odd.

a. Assume, to the contrary, that $\sqrt{2} = u/v$, in lowest terms, for some $u, v \in \mathbb{N}^+$. Then $u^2 = 2v^2$, which is even. Therefore, u is even. Let $u = 2w$, where $w \in \mathbb{N}^+$. We get

$$(2w)^2 = 2v^2\,, \quad \text{i.e., } v^2 = 2w^2\,,$$

which is even. Therefore, v is even. Since u and v are both even, the expression u/v is not in lowest terms, a contradiction.

b. Suppose that $p \mid n^2 = n \cdot n$. Applying Euclid's Lemma (the "consequently" portion), we directly get $p \mid n$.

c. Let p be an arbitrary prime. Assume, to the contrary, that $\sqrt{p} = u/v$, in lowest terms, for some $u, v \in \mathbb{N}^+$. Then $u^2 = pv^2$, so $p \mid u^2$, so $p \mid u$ (by the previous part). Let $u = pw$, where $w \in \mathbb{N}^+$. We get

$$(pw)^2 = pv^2\,, \quad \text{i.e., } v^2 = pw^2\,,$$

which means $p \mid v^2$. Therefore, $p \mid v$. Since p divides both u and v, the expression u/v is not in lowest terms, a contradiction.

d. Suppose that $p \mid n^2 = n \cdot n$. Applying Euclid's lemma (the "consequently" portion), we directly get $p \mid n$.

e. Let p be an arbitrary prime and $a \in \mathbb{Z}$. By repeatedly using Euclid's Lemma, we get that

$$\begin{aligned} p \mid a^n = a \cdot a^{n-1} &\implies \text{either } p \mid a \text{ or } p \mid a^{n-1} = a \cdot a^{n-2} \\ &\implies \text{either } p \mid a \text{ or } p \mid a^{n-2} = a \cdot a^{n-3} \\ &\implies \cdots \\ &\implies \text{either } p \mid a \text{ or } p \mid a\,. \end{aligned}$$

In short, $p \mid a^n \implies p \mid a$.

Now let n be an arbitrary integer ≥ 2. Assume, to the contrary, that $p^{1/n} = u/v$, in lowest terms, for some $u, v \in \mathbb{N}^+$. Then $u^n = pv^n$, so $p \mid u^n$, so $p \mid u$ (by the above). Let $u = pw$, where $w \in \mathbb{N}^+$. We get

$$(pw)^n = pv^n\,, \quad \text{i.e., } v^n = p^{n-1}w^n\,.$$

Since $n \geq 2$, this means $p \mid v^n$. Therefore, $p \mid v$. Since p divides both u and v, the expression u/v is not in lowest terms, a contradiction.

Solution for PS5-9.

a. The numbers 1 and $p-1$ (which are distinct because $p \geq 3$) are self-inverses, because $1^2 \equiv 1 \pmod{p}$ and $(p-1)^2 \equiv (-1)^2 \equiv 1 \pmod{p}$. To show that there are no others, suppose $a \in \mathbb{Z}_p$ is a self-inverse, so $a^2 \equiv 1 \pmod{p}$. By the definition of congruence,

$$p \mid a^2 - 1 = (a-1)(a+1)\,.$$

By Euclid's Lemma, either $p \mid a-1$ or $p \mid a+1$, i.e., either $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.

b. We can solve this by exhaustive case analysis, but let's be cleverer. Reasoning as above, 1 and 14 are clearly self-inverses. Further, if $a^2 \equiv 1 \pmod{15}$, then

$$15 \mid a^2 - 1 = (a-1)(a+1) \quad \implies \quad 5 \mid (a-1)(a+1)\,.$$

So $a \equiv \pm 1 \pmod{5}$. Besides 1 and 14, the only other values in $\mathbb{Z}_{15}$ satisfying this are $4, 6, 9$, and 11. But by analogous reasoning, $a \equiv \pm 1 \pmod{3}$, so we can eliminate 6 and 9. Finally, $4^2 \equiv 11^2 \equiv 1 \pmod{15}$.

Thus, there are exactly four self-inverses modulo 15: they are $1, 4, 11$, and 14.