18.781 Solutions to Problem Set 1

1. Suppose not. Then let S be the set of integers $\{-(b+ka) : k \in \mathbb{Z}\}$, so by hypothesis S consists entirely of nonnegative integers. By the Well-Ordering Principle, it has a smallest positive element, say, $b+ka$. But then $b+(k-1)a$ is smaller since $a > 0$, contradiction.

2. The largest such integer is $ab-a-b$. To see it's not a nonnegative integer linear combination, suppose $ab-a-b = ax+by$ with $x, y \in \mathbb{Z}_{\geq 0}$. Then $a(b-1-x) = b(y+1)$. And since $(a,b) = 1$ we have $a|y+1$ (and $b|b-1-x$). This forces $y \geq a-1$ because $y+1 \geq 1$. So

   $$ax + by \geq a \cdot 0 + b(a-1) = ab - b > ab - a - b,$$

   contradicting $ab - a - b = ax + by$.

   On the other hand, suppose $n > ab-a-b$. Since $\gcd(a,b) = 1$ we can write $n = ax+by$ with $x, y \in \mathbb{Z}$ (not necessarily nonnegative). Now note that $n = a(x-bk) + b(y+ak)$ for any integer k. By the division algorithm, there exists an integer k such that $0 \leq x - bk < b$. Let $x' = x - bk$ and $y' = y + ak$. Then we have $n = ax' + by'$ with $0 \leq x' \leq b-1$, so

   $$by' = n - ax' \geq (ab - a - b + 1) - a(b-1) = -(b-1).$$

   Therefore $y' \geq \frac{-(b-1)}{b}$, and since y' is an integer, we get $y' \geq 0$. This shows that $n = ax' + by'$ is a nonnegative integer linear combination.

3. One direction is clear: if $m|n$ then $n = mk$ for some positive integer k, and

   $$a^n - 1 = a^{mk} - 1 = (a^m - 1)(a^{m(k-1)} + a^{m(k-2)} + \cdots + a^m + 1)$$

   is divisible by $a^m - 1$. Now if $m \nmid n$, we write $n = mk + r$ with $0 < r < m$. Then

   $$a^n - 1 = a^{mk+r} - 1 = a^{mk+r} - a^r + a^r - 1 = a^r(a^{mk} - 1) + a^r - 1.$$

   Now $a^m - 1$ divides $a^{mk} - 1$ but it doesn't divide $a^r - 1$, since $0 < a^r - 1 < a^m - 1$. So $a^m - 1$ can't divide $a^n - 1$.

4. Using the Euclidean algorithm:

	89	1	0
2	43	0	1
14	3	1	−2
	1	−14	29

   So $(-14)89 + (29)43 = 1$, i.e., $(x_0, y_0) = (-14, 29)$. Now if x, y is any solution then $89(x-x_0) + 43(y-y_0) = 0$. And since 43 and 89 are coprime, $43|x_0 - x$ and $89|y - y_0$. Then we have

   $$\begin{cases} x = x_0 - 43k \\ y = y_0 + 89k \end{cases}$$

   for some $k \in \mathbb{Z}$. It's easy to verify that all solutions of this form satisfy $89x + 43y = 1$. So all the solutions are given by

   $$(x, y) \in \{(-14 - 43k, 29 + 89k) : k \in \mathbb{Z}\}.$$

5. Since $1 < a < b$,
$$\begin{cases} b = aq + r & 0 < r < a \\ a = rq' + s & 0 \leq s < r. \end{cases}$$
(If $r = 0$ we're done in one step.) So after two steps, (a, b) gets replaced by (s, r). We claim $s < a/2$. If in step 1, $r \leq a/2$, then we're done by $s < r$. Otherwise, $r > a/2$ and in step 2 we'll have $q' = 1$ and $s = a - r < a/2$. In any case, we see that after two steps, the value of a at least halves. So after at most $2\log_2 a$ steps, we'll get a pair $(a_{\text{new}}, b_{\text{new}})$ such that $a_{\text{new}} < 2$, i.e., $a_{\text{new}} = 1$. Therefore the algorithm terminates after at most $C \log a$ steps for $C = 2/\log 2$.

6. You should notice that about 50% of the primes are 1 mod 4 and about 50% are 3 mod 4. Also, the number of primes which are 3 mod 4 seems to be larger than the number of primes 1 mod 4, up to any integer. This is not always the case—see the article "Prime number races" by Andrew Gronville and Greg Martin for a fascinating account.

7. A can always win.

   Proof: Note that for any fixed n, there are only finitely many squares on the board, so it's a finite game, which means that one of the players must have a winning strategy. If B has a winning strategy, we'll show a contradiction. Since A puts down the first token, A can choose to put it down on the square 1. Then B must have a winning strategy from here, so suppose B puts down a token on square k. However, A could start with k instead, and imitate what B would have done (B can't use 1, since 1 divides k). This shows that A wins if starting with k, contradiction.

   Note: I don't know of an explicit winning strategy; that problem seems to be unsolved!

8. We use proof by contradiction, as in Euclid's proof. Suppose there are only finitely many primes of the form $4k + 3$, say, $p_1, \ldots, p_n$. Now consider
$$N = 4p_1 \cdots p_n - 1.$$
Clearly $N > 1$, and $N \equiv 3 \bmod 4$. So N must have a prime divisor congruent to 3 mod 4, else if all the factors of N are congruent to 1 mod 4 then $N \equiv 1 \pmod 4$. But then some p_i must divide N, a contradiction since $p_i | 4p_1 \cdots p_n$ and $p_i \nmid 1$.

18.781 Theory of Numbers
Spring 2012