Math 163 Introductory Seminar - Lehigh University - Spring 2008 - Assignment 5 Solutions
Due Wednesday February 20

12. (a) If b is a 99 digit number how many bits are needed to represent it? That is, if b is a 99 digit number, how many digits are needed when it is represented base 2? Your answer will be a range of several numbers. Consider how $\log$ (common logarithm, base 10) and $\lg$ (logarithm base 2) relate to the number of digits. Use this and basic facts about logarithms. We have not discussed basic rules for logarithm manipulation in class. If you do not recall these use any inanimate source that you like.
(b) Answer as in part (a) except for a $t-1$ digit number. Your answer should be a range of numbers specified by two values written in terms of t and some logarithms.

Note that b has $t-1$ digits if $t-2 \leq \log b < t-1$. So b has $\lfloor \log b \rfloor + 1$ digits where $\lfloor x \rfloor$ is the floor function which is the largest integer less than or equal to x. Similarly the number of bits needed to represent b is $\lfloor \lg b \rfloor + 1$. A basic logarithm identity is $\log_a b = \frac{\log_c b}{\log_c a}$. So in particular we have $\log_{10} b = \frac{\log_2 b}{\log_2 a}$. Using log for log base 10 and lg for log base 2 we get $\log b = \frac{\lg b}{\lg 10}$. If b has 99 digits then $98 \leq \log b < 99$. Substituting this gives $98 \cdot \lg 10 \leq \lg b < 99 \lg 10$ with $\lg 10 \approx 3.32193$ we get (approximately) $325.54 \leq \lg b < 328.86$. So is has between 326 and 329 bits. Replacing 98 and 99 above with $t-2$ and $t-1$ we get that $(t-2) \cdot \lg 10 \leq \lg b < (t-1) \cdot \lg 10$ or (approximately) $(t-2) \cdot 3.32193 \leq \lg b < (t-1) \cdot 3.32193$. The number of bits is between $\lfloor (t-2) \cdot \lg 10 \rfloor + 1$ and $\lfloor (t-1) \cdot \lg 10 \rfloor + 1$. (If $(t-1) \cdot \lg 10$ was an integer we would need $\lfloor (t-1) \cdot \lg 10 \rfloor$ bits instead of $\lfloor (t-1) \cdot \lg 10 \rfloor + 1$ but since $\lg 10$ is irrational this will never happen so the bound $\lfloor (t-1) \cdot \lg 10 \rfloor + 1$ is correct for all t.)

13. What is the smallest k such that the Fibonacci number F_k has at least 99 digits? What does this tell you about the number of steps in the Euclidean algorithm in the worst case if the smaller of the two numbers for which you determine the gcd has 99 digits? Recall that F_k is the integer closest to $\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^k$. As in the previous problem, think about how the number of digits relates to the common logarithm and find and use some basic facts about logarithms.

As in the previous problem we need the smallest k such that $\log F_k \geq 98$. Using $F_k \approx \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^k$ along with the basic log identities $\log ab = \log a + \log b$ and $\log b^k = k \log b$ we get $\log\left(\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^k\right) = \log \frac{1}{\sqrt{5}} + k \log \frac{1+\sqrt{5}}{2}$. With $\log \frac{1}{\sqrt{5}} \approx .34948$ and $\log \frac{1+\sqrt{5}}{2} \approx .208988$ we get $\log \frac{1}{\sqrt{5}} + k \log \frac{1+\sqrt{5}}{2} \geq 98$ when (approximately) $k \geq 470.59$. This expression is less than 98 when $k \leq 470$ and at least 98 when $k \geq 471$. Observe that with $F_k = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^k - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^k$ we get that $\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^k$ is an overestimate of F_k when k is even and and underestimate when k is odd. So our computations showing $\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^k$ with $k = 471$ is at least 10^{98} and with $k = 470$ is less than 10^{98} show that F_{471} has at least 99 digits and that F_{470} has at most 98 digits.

14. Prove that for positive integers $a_1, a_2, \ldots, a_k, c$ we have that $a_1x_1 + a_2x_2 + \cdots + a_kx_k = c$ has a an integer solution only if c is a multiple of the greatest common divisor $\gcd(a_1, \ldots, a_k)$ of the a_i.

We need to show that if there is an integer solution then c is a multiple of $\gcd(a_1, \ldots, a_k)$. Let $g = \gcd(a_1, \ldots, a_k)$ then for $i = 1, 2 \ldots, k$ there exist integers h_i with $a_i = gh_i$ since g divides each of the a_i. If $x_1^*, x_2^*, \ldots, x_k^*$ satisfy $a_1x_1^* + a_2x_2^* + \cdots + a_kx_k^* = c$ then substituting $a_i = gh_i$ we get $g(h_1x_1^* + h_2x_2^* + \cdots + h_k) = a_1x_1^* + a_2x_2^* + \cdots + a_kx_k^* = c$. Since $(h_1x_1^* + h_2x_2^* + \cdots + h_k)$ is an integer, c is a multiple of $g = \gcd(a_1, \ldots, a_k)$.

15. Prove that for positive integers $a_1, a_2, \ldots, a_k, c$ we have that $a_1x_1 + a_2x_2 + \cdots + a_kx_k = c$ has a an integer solution if c is a multiple of the greatest common divisor $\gcd(a_1, \ldots, a_k)$ of the a_i. Note that it is enough to show that there is a a solution when $c = \gcd(a_1, \ldots, a_k)$ and then use induction on k. You may use the $k = 2$ case proved in class as a basis. You may also use the fact that $\gcd(\gcd(a_1, \ldots, a_{k-1}), a_k) = \gcd(a_1, \ldots, a_k)$.

We need to show that if c is a multiple of $\gcd(a_1, \ldots, a_k)$ then there is an integral solution. We assume that we have shown the basis for the induction, $a_1x_1 + a_2x_2 = c$ has an integer solution if c is a multiple of $\gcd(a_1, a_2)$. It is enough to show that there is a solution for $g = \gcd(a_1, \ldots, a_k)$ since if c is a multiple of g, then $c = qg$ for some integer q and if $x_1^*, x_2^*, \ldots, x_k^*$ are integers satisfying $a_1x_1^* + a_2x_2^* + \cdots + a_kx_k^* = g$ then $qx_1^*, qx_2^*, \ldots, qx_k^*$ satisfy $a_1(qx_1^*) + a_2(qx_2^*) + \cdots + a_k(qx_k^*) = qg = c$. Now assume $k \geq 3$. Let $g' = \gcd(a_1, a_2, \ldots, a_{k-1})$. By induction we can assume that there exists integers $v_1^*, v_2^*, \ldots, v_{k-1}^*$ satisfying $a_1v_1^* + a_2v_2^* + \cdots + a_{k-1}v_{k-1}^* = \gcd(a_1, \ldots, a_{k-1}) = g'$ and that there exist integers w_1^*, w_2^* satisfying $g'w_1^* + a_kw_2^* = \gcd(g', a_k) = \gcd(\gcd(a_1, \ldots, a_{k-1}), a_k) = \gcd(a_1, a_2, \ldots, a_k) = g$. Then $x_i^* = w_1^*v_i^*$ for $i = 1, \ldots, k-1$ and $x_k = w_2^*$ are integers satisfying $a_1x_1^* + a_2x_2^* + \cdots + a_{k-1}x_{k-1}^* + a_kx_k^* = (a_1v_1^* + a_2v_2^* + \cdots + a_{k-1}v_{k-1}^*)w_1^* + a_kw_2^* = g'w_1^* + a_kw_2^* = g$. So by induction there is an integer solution when $c = g$ and from the remarks above when c is a multiple of g.

16. Consider the statement that exactly one of the following holds for given integers: $a_1, a_2, \ldots, a_k, c$: (I) $a_1x_1 + \cdots + a_kx_k = c$ has an integer solution $x_1, x_2, \ldots, x_k$; (II) ya_i integral for $i = 1, 2, \ldots, k$ and yc non-integral has a solution y.
Prove directly that at most one of (I) or (II) holds.

Assume that both hold. That is, there exist integers $x_1^*, x_2^*, \ldots, x_k^*$ with $a_1x_1^* + \cdots + a_kx_k^* = c$ and a number y^* with ya_i an integer for $i = 1, 2, \ldots, k$ and y^*c not an integer. Then $y^*c = y^*(a_1x_1^* + \cdots + a_kx_k^*) = y^*a_1x_1^* + y^*a_2x_2^* + \cdots + y^*a_kx_k^*$ is an integer since y^*a_i and x_i^* are both integers. This a contradiction, so at most one of (I) or (II) can hold.

17. Consider the statement that exactly one of the following holds for given integers: $a_1, a_2, \ldots, a_k, c$: (I) $a_1x_1 + \cdots + a_kx_k = c$ has an integer solution $x_1, x_2, \ldots, x_k$; (II) ya_i integral for $i = 1, 2, \ldots, k$ and yc non-integral has a solution y.
This is really just a restatement of 14 and 15 above. Show this statement using those results. By 16 it is enough to show that at least one holds. Consider two cases, whether or not c is a multiple of $\gcd(a_1, \ldots, a_k)$ and explain why (using 14 or 15) this gives a solution in (I) or (II).

From problem 16, at most one of (I) or (II) holds. If c is a multiple of $\gcd(a_1, a_2, \ldots, a_k)$ then by problem 15 (I) holds. If c is not a multiple of $g = \gcd(a_1, \ldots, a_k)$ then let $y^* = \frac{1}{g}$. Since c is not a multiple g, y^*g is not an integer. Since a_i is a multiple of g for $i = 1, 2, \ldots, k$, $y^*a_i = \frac{a_i}{g}$ is an integer for $i = 1, 2 \ldots, k$. Thus (II) has a solution.