Math 445 Homework 3

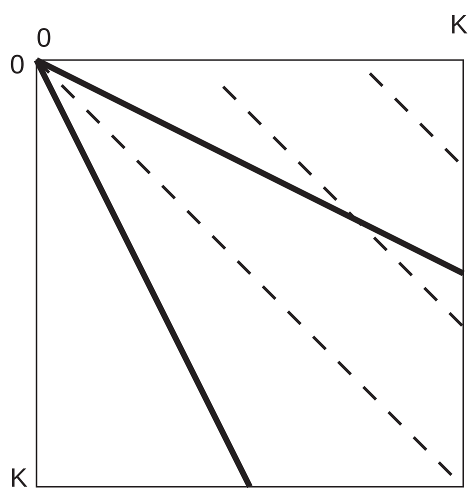
Due Friday, Sept. 27

9. Our description of RSA assumed that for $n = pq$, that $(a, n) = 1$. But we don't control a, the sender does! Show that in any event, the RSA algorithm works even if $(A, n) > 1$:

   Show that if $n = pq$ is a product of distinct primes and $de \equiv 1 \pmod{(p-1)(q-1)}$, then $a^{de} \equiv a \pmod{n}$ for <u>any</u> a.

   (Hint: show that it works mod p and q, first.)

10. Our argument for"square root of work for half the chance of success" in the Pollard ρ method was a little imprecise; make a better estimate of the number of starting points in a $K \times K$ grid whose lines of slope -1 will hit the "success" lines of slope $-1/2, -2$ emanating from $(0, 0)$, to make a better estimate of the fraction of success we are trading less work for. (Note: lines starting from the upper right/lower left corners may miss the success lines before we stop computing $(a_i - a_{2i}, n)$.)



11. [NZM p.83, # 13] When applying the Pollard ρ method, starting from a_1, suppose we find that $a_i - a_j$, for $1 \leq i \neq j \leq 17$, are coprime to n, but then $a_{18} - a_{11}$ shares a factor with n. What is the smallest k that we then <u>know</u> of that will have $a_{2k} - a_k$ sharing a factor with n?

12. [NZM p.83, # 15] Show that if $(a, m) = 1$ and there is a prime p with $p|m$ and $(p-1)|Q$, then $(a^Q - 1, m) > 1$.