Math 445 Homework 3 Solutions

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.

   We'll show that $A^{de} \equiv A \pmod{p}$ and $A^{de} \equiv A \pmod{q}$, i.e., p and q both divide $A^{de} - A$. Then since p and q are distinct primes, $(p, q) = 1$, and so $n = pq | A^{de} - A$.

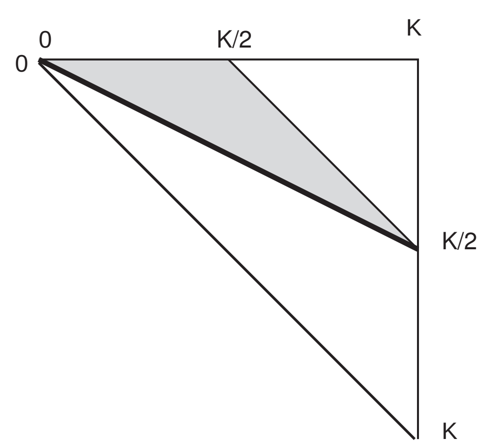
   By hypothesis, $de - 1 = k(p-1)(q-1)$, so $de = 1 + k(p-1)(q-1)$. Given A, one of three things is true: (1) $(A, p) = (A, q) = 1$, (2) exactly one of p, q divides A, WOLOG $p|A$ (since there is no distinction between them) and $(A, q) = 1$, or (3) $p, q|A$, so $n = pq|A$.

   In case (1), Fermat's Little Theorem tells us that $A^{p-1} \equiv 1 \pmod{p}$ and $A^{q-1} \equiv 1 \pmod{q}$, so $A^{de} = (A^{p-1})^{k(q-1)}A \equiv 1^{k(q-1)}A \equiv A \pmod{p}$ and $A^{de} = (A^{q-1})^{k(p-1)}A \equiv 1^{k(p-1)}A \equiv A \pmod{q}$ as desired. In case (2), $A \equiv 0 \pmod{p}$, so $A^{de} \equiv 0^{de} \equiv 0 \equiv A \pmod{p}$, while, as in (1), $A^{de} \equiv A \pmod{q}$. Finally, in case (3), $A \equiv 0 \pmod{p}$ and $A \equiv 0 \pmod{q}$, so $A^{de} \equiv 0^{de} \equiv 0 \equiv A \pmod{p}$ and the same for q . So in all cases, $A^{de} \equiv A \pmod{p}$ and $\pmod{q}$, so $A^{de} \equiv A \pmod{n}$.

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 $(a_i - a_{2i}, n)$.)

    We know that if $(a_j - a_i, n) > 1$, then $(a_{j+k} - a_{i+k}, n) > 1$ for all $k \geq 0$. If we focus on the set of pairs (j, i) with $1 \leq i, j \leq K$ and $j > i$, we wish to estimate the sie of the set of such points for which the sequence of pairs $(j+k, i+k)$ intersects the sequence of pairs $(2m, m)$ <u>before</u> m exceeds K. [By setting $j > i$, we will work with the upper right half of the $K \times K$ square, the other half would interact with the "line" of pairs $(m, 2m)$, instead, and give an identical estimate.]

    But the set of pairs whose line of successors meet the $(2m, m)$ line inside of the $K \times K$ square are precisely the points lying in the triangle of points lying up the slope -1 lines from the line $x + 2y = 0$ of slope -1/2 emanating from the origin $(0, 0)$; see the figure below. We need to determine what fraction of the pairs (j, i) above the line $x + y = 0$ lie in that triangle. But this is a matter of computing areas:



The triangle of all pairs (j,i) has base K and height K, so has area $B = K \cdot K/2 = K^2/2$. The traingle of all pairs whose slope -1 lines will meet our success line (the shaded triangle above) has base $K/2$ and height $K/2$, so has area $(K/2)(K/2)/2 = K^2/8$. So the fraction of pairs that could be detected by our success line is $(K^2/8)/(K^2/2) = 1/4$. So roughly 1/4 of the pairs we could test and find $(a_j - a_i, n) > 1$ wuld be detected by instead testing for $(a_{2i} - a_i, n) > 1$. So we have 1/4 the chance of succeeding (over testing <u>all</u> pairs) by doing roughly square root (test K pairs, instead of $K(K-1)/2$ pairs) work. Which for large K is a very good trade-off!

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?

    Essentially, we are asking: what is the smallest k so that $(2k, k) = (18+m, 11+m)$ for some $m \geq 0$? We therefore want

    $2k = 18 + m$, $k = 11 + m$, which, subtracting, gives $k = 7$. But this is ridiculous; this yields the point $(14, 7)$ which is <u>behind</u> $(18, 11)$, and we <u>can't</u> conclude that $(a_{14} - a_7, n) > 1$. My bad.

    But as the text points out, we know that even more is true: if we set $d = (a_{18} - a_{11}, n)$, then $a_{18} \equiv a_{11} \pmod{d}$, so $a_{18+k} \equiv a_{11+k} \pmod{d}$ for every $k \geq 0$. But when $k = 7$, this gives $a_{25} \equiv a_{18} \equiv a_{11}$, and so $a_{25+k} \equiv a_{11+k}$ as well. Essentially, after $r = 11$, a_k cycles through 7 values mod d, i.e., $a_{11+j+7k} \equiv a_{11+j+7l}$ for every $0 \leq j \leq 6$ and $k, l \geq 0$. So to find an i for which $d|a_{2i} - a_i$, so (since $d|n$) $d|(a_{2i} - a_i, n)$ and $(a_{2i} - a_i, n) > 1$, we need to find an i so that $2i = 11 + j + 7l$ and $i = 11 + j + 7k$ for some j, k, and l. Subtracting, we get $i = 7(l-k)$. The smallest i will be when $k = 0$ (i.e., $i = 11 + j + 7k$ is in the first round of cycling), so we need $i = 7l$ and $i = 11 + j$ with $0 \leq j \leq 6$, so $j = 3$ and $i = 14$, $2i = 28$. So $(a_{28} - a_{14}, n) > 1$ giving, usually, a proper factor of n.

    In the end, since $18 - 11 = 7$, we seek a pair $(2i, i)$ with $2i \geq 18$, $i \geq 11$, and $2i - i = i$ a multiple of 7; the first such i is $i = 14$.

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 $(a^Q - 1, m) > 1$.

    We show, in fact, that $p|^Q - 1, m)$, so $(a^Q - 1, m) \geq p > 1$. We know, by hypothesis, that $p|m$, so it is enough to show that $p|A^Q - 1$. But since $p - 1|Q$, $Q = (p-1)k$ for some k, and then $a^Q = a^{(p-1)k} = (a^{p-1})^k \equiv 1^k = 1 \pmod{p}$, by Fermat's Little Theorem, so $p|(a^{p-1})^k - 1 = a^Q - 1$, as desired. So $(a^Q - 1, m) \geq p > 1$.

    [N.B. This fact is the basis for Pollard's $p - 1$ Test: if m has a prime factor such that $p - 1$ is a product of "small" primes, then $(p-1)|N!$ for some relatively small value of N, so, e.g., $(2^{N!} - 1, m) > 1$ can be computed relatively quickly, usually finding a factor of m. In most implementations of RSA, for example, the program generates industrial-grade primes p, q, but also checks that $(p-1), (q-1)$ each have at least one large prime factor, to protect against this method of finding a factor of $m = pq$.]