Homework 33, due December 1

(1) We show how to quickly compute discrete logarithms mod p, assuming we have access to a certain period-finding oracle. Shor's algorithm for discrete logarithms essentially turns a quantum computer into this period-finding oracle.

Throughout the problem, p is an odd prime such that $p-1=2q$, where q is also an odd prime. We let α be a primitive root mod p, and $\beta \equiv \alpha^x \pmod{p}$ for some secret x we wish to find. We may assume $1 \leq x < p-1$.

(a) Recall an order-finding oracle mod N instantly returns the order r of $a \pmod{N}$ when given a (the order r is the least positive integer such that $a^r \equiv 1 \pmod{N}$). Show that $f(x) = a^x \pmod{N}$ is periodic with period r, i.e., that $f(x+r) \equiv f(x) \pmod{N}$ for every x.

(b) Define a two-variable function $f(r,s) = \alpha^r \beta^s \pmod{p}$. Show there exist nonzero $w_1, w_2 \pmod{p-1}$ such that $f(r+w_1, s+w_2) \equiv f(r,s) \pmod{p}$ for every r, s. (Hint: Show that $f(r+w_1, s+w_2) \equiv f(r,s) \pmod{p}$ if and only if $\alpha^{w_1+xw_2} \equiv 1 \pmod{p}$. Prove this latter condition holds if and only if $w_1+xw_2 \equiv 0 \pmod{p-1}$. Choose any $w_2 \not\equiv 0 \pmod{p-1}$, and take $w_1 \equiv -xw_2 \pmod{p-1}$.)

(c) Assume we have a period-finding oracle, which gives us nonzero $w_1, w_2 \pmod{p-1}$ such that $f(r+w_1, s+w_2) \equiv f(r,s) \pmod{p}$ for all r, s. Show that we can quickly find x if $q \nmid w_1 w_2$. (Hint: By arguing similarly to part (b), show that $w_1 + xw_2 \equiv 0 \pmod{p-1}$. This implies $w_1 + xw_2 \equiv 0 \pmod{q}$. Prove that one can find $x \pmod{q}$ in terms of w_1, w_2. Explain how to use this to find $x \pmod{p-1}$.)

(d) Prove that $\alpha^q \equiv -1 \pmod{p}$. Explain why we can assume $q \nmid x$.

(e) Show that if $q \mid w_1$ or $q \mid w_2$, then $q \mid w_1$ and $q \mid w_2$. Show this implies $w_1 = w_2 = q$.

(f) Assume that $f(r+q, s+q) \equiv f(r,s) \pmod{p}$ for every r, s. Show that $(-1)^x \equiv -1 \pmod{p}$.

(g) Assume that $f(r+q, s+q) \equiv f(r,s) \pmod{p}$ for every r, s. Given a positive integer e, define $\beta_1 \equiv \beta\alpha^e$. Further define

$$f_1(u,v) \equiv \alpha^u \beta_1^v \pmod{p},$$

and assume we use the period-finding oracle to give us nonzero $z_1, z_2 \pmod{p-1}$ such that $f_1(u+z_1, v+z_2) \equiv f_1(u,v) \pmod{p}$ for every u, v. Show that, if e is odd, then $q \nmid z_2$. (Hint: Use proof by contradiction and part (f).) Deduce that we can quickly find $x \pmod{q}$ and therefore $x \pmod{p-1}$. Conclude that, in any case, we can always solve the discrete logarithm problem mod p assuming we have access to the period-finding oracle.

(2) Read sections 18.1-18.2 of Boaz Barak's Quantum Computing and Cryptography I. Make sure to stop and do his blue "pause and think" boxes. Write a few thoughts about what you read.