Lecture 10 Pollard's $p-1$ Factorization Algorithm

For numbers of the form $n = pq$ as used in RSA, we wish to be able to efficiently factor n.
Suppose there is a number L such that $p-1 \mid L,\ q-1 \nmid L$. Then $L = i(p-1),\ L = j(q-1)+k,\ \ k \neq 0$.

Then for any integer a relatively prime to n.

$$a^L \equiv a^{i(p-1)} \equiv (a^{p-1})^i \equiv 1^i \equiv 1 \pmod{p}$$

$$a^L \equiv a^{j(q-1)+k} \equiv (a^{q-1})^j a^k \equiv a^k \pmod{q}$$

It is highly unlikely that $a^k \equiv 1 \pmod{q}$. Sothe above congruences most likely impythat $p \mid a^L - 1,\ q \nmid a^L - 1$. If this is the case then $p = \gcd(a^L - 1, n)$ and we will then be able to factor n.

To be able to factor n we must choose a convenient value for L. If we are lucky and $p-1$ has relatively small prime factors then we can use $L = n!$ for small values of n.

Pollard $p-1$ Algorithm
Step 1: Let $a = 2$ (in general use a value of a that is relatively prime to n)
Step 2: For $j = 2, 3, \ldots$ up to some predetermined upper bound
Step 3: Let $a = a^j \pmod{n}$
Step 4: Let $d = \gcd(a-1, n)$
Step 5: If $1 < d < n$ then d is a factor of n.

Note: If this doesn't work one can try a different value of a.

Examples
(1) $n = 319$. Start with $a = 2, j = 2$

$$2^{2!} \equiv 4 \pmod{319},\ \ \gcd(3, 319) = 1$$

$$2^{3!} \equiv 64 \pmod{319},\ \gcd(63, 319) = 1$$

$$2^{4!} \equiv 49 \pmod{319},\ \gcd(48, 319) = 1$$

$$2^{5!} \equiv 111 \pmod{319},\ \gcd(110, 319) = 11$$

Let $p = 11,\ q = n/p = 29$, we have factored n.

(2) $n = 12759787$. Start with $a = 2,\ j = 5$

$$2^{5!} \equiv 5215267 \pmod{n},\ \ \gcd(5215266, n) = 1$$

$$2^{6!} \equiv 5262262 \pmod{n},\ \ \gcd(5262261, n) = 1$$

$$2^{7!} \equiv 8444743 \pmod{n},\ \gcd(8444742, n) = 1$$

$$2^{8!} \equiv 3474286 \pmod{n},\ \gcd(3474285, n) = 3457$$

Let $p = 3457,\ q = n/p = 3691$, we have factored n.