Review

Square roots modulo primes:
(exactly two square roots of b^2)

Sun-Ze theorem to solve simultaneous equations with $\gcd(m,n) = 1$

$$\begin{cases} x = a \bmod m \\ x = b \bmod n \end{cases}$$

Compute via Euclid.

Square roots modulo composites:
(exactly four square roots of b^2 modulo $p \cdot q$ with distinct primes p, q)

Square root oracle and factoring $p \cdot q$

Pollard's rho factorization attack

Pollard's $p - 1$ factorization attack

We continue to look at ways in which composite integers are different from primes.

Primality testing seems to be much easier than *factoring.* This helps make RSA and other PK ciphers feasible and (apparently) secure.

Miller-Rabin *pseudoprime test* is about as good as one could wish.

There are much better *factorization attacks* than trial division, such as Pollard's rho and various **sieve** methods (quadratic sieve, number field sieve), but these are still much slower than primality testing.

Other clever PK protocols make further use of number theory.

Polynomial algebra mod primes

In high school algebra we learn that a polynomial equation $f(x) = 0$ has no more roots than the degree of the polynomial f.

For example, a quadratic polynomial will have at most two roots.

This is still true if we consider polynomials with coefficients in $\mathbf{Z}/p$ and look for roots in $\mathbf{Z}/p$, for p a *prime*.

This generalizes the issue of square roots, solving $x^2 - b^2 = 0 \bmod p$.

This will fail for composite moduli, just as there were more than two square roots for composite moduli.

Proposition: A quadratic equation has at most two roots modulo a prime p.

Proof: Suppose a is a root of $f(x) = 0 \bmod p$ where $f(x) = x^2 + Ax + B$. Divide the polynomial $x^2 + Ax + B$ by $x - a$ in steps

$$(x^2 + Ax + B) - x \cdot (x - a) = (A + a)x + B$$

$$((A + a)x + B) - (A + a)(x - a) = a^2 + Aa + B$$

to get

$$x^2 + Ax + B = (x + (A + a)) \cdot (x - a) + r$$

where $r = a^2 + Aa + B$ is a constant (in $\mathbf{Z}/p$). Not surprisingly, this constant is the value $f(a)$ of the original polynomial at $x = a$. Thus, as for polynomials with rational, real, or complex coefficients, $f(a) = 0$ if and only if $x - a$ divides $f(x)$.

Then for $f(a) = 0$

we see that

$$x^2 + Ax + B = (x - a)(x - (-A - a))$$

so another root is $-A - a$. For brevity let $b = -A - a$, so

$$f(x) = (x - a)(x - b)$$

Now we show that there is no *other* root than a and b. Suppose $f(c) = 0$. Then

$$(c - a)(c - b) = 0 \bmod p$$

That is, $p|(c - a)(c - b)$. Because p is *prime*, if $p|st$ then $p|s$ or $p|t$. Thus, either $p|(c - a)$ or $p|(c - b)$. That is, either $c = a \bmod p$ or $c = b \bmod p$.

Thus, there are at most two roots to a quadratic equation modulo a prime.

///

Non-unique factorization mod composites

Modulo composites polynomial equations will typically have more than the expected number of solutions, *and*, the polynomials themselves factor in more than one way.

For example

$$x^2 - 3x + 2 = (x - 1)(x - 2) \bmod 15$$

showing the two roots 1 and 2 of

$$x^2 - 3x + 2 = 0 \bmod 15$$

But also

$7^2 - 3 \cdot 7 + 2 = 49 - 21 + 2 = 30 = 0 \bmod 15$

$11^2 - 3 \cdot 11 + 2 = 121 - 33 + 2 = 90 = 0 \bmod 15$

and there is *another* factorization

$$x^2 - 3x + 2 = (x - 7)(x - 11) \bmod 15$$

Non-unique factorization of quadratic polynomials is understood via Sun-Ze's theorem. For t to be a root of $(x-a)(x-b) = 0 \bmod pq$ with distinct primes p and q it is necessary and sufficient that

$$\begin{cases} (t-a)(t-b) = 0 \bmod p \\ (t-a)(t-b) = 0 \bmod q \end{cases}$$

equivalently

$$\begin{cases} t = a \text{ or } b \bmod p \\ t = a \text{ or } b \bmod q \end{cases}$$

The obvious choices are $t = a \bmod$ both p and q, and $t = b \bmod$ both p and q. The *mismatched* choices

$$t_3 = a \bmod p \text{ and } t_3 = b \bmod q$$

or

$$t_4 = b \bmod p \text{ and } t_4 = a \bmod q$$

give two more roots. Also another factorization

$$(x-a)(x-b) = (x-t_3)(x-t_4) \bmod pq$$

For example, to factor $(x-3)(x-5) \bmod 77$ in another way, note that (by trial division) 77 factors into primes $77 = 7 \cdot 11$ and $(x-3)(x-5) = 0 \bmod 77$ is equivalent to

$$\begin{cases} (x-3)(x-5) = 0 \bmod 7 \\ (x-3)(x-5) = 0 \bmod 11 \end{cases}$$

or

$$\begin{cases} x = 3 \text{ or } 5 \bmod 7 \\ x = 3 \text{ or } 5 \bmod 11 \end{cases}$$

The non-obvious solutions are the mismatched ones

$$t_3 = 3 \bmod 7 \text{ and } t_3 = 5 \bmod 11$$
$$t_4 = 5 \bmod 7 \text{ and } t_4 = 3 \bmod 11$$
$$cr$$

By Euclid $1 = 2 \cdot 11 - 3 \cdot 7$, and by Sun-Ze

$$t_3 = (2 \cdot 11) \cdot 5 - (3 \cdot 7) \cdot 3 = 47 \bmod 77$$
$$t_4 = (2 \cdot 11) \cdot 3 - (3 \cdot 7) \cdot 5 = 38 \bmod 77$$

And also

$$(x-3)(x-5) = (x-38)(x-47) \bmod 77$$

Hensel's Lemma

So far our discussion of composite moduli has ignored the possibility that a modulus has a factor of p^2 or p^3 or a higher power of a prime.

Sun-Ze's theorem does *not* get us from a solution mod p to a solution mod p^2, for example.

For general modulus $m = p_1^{e_1} \ldots p_t^{e_t}$ we would need to solve separately modulo the prime *powers* $p_1^{e_1}, \ldots, p_t^{e_t}$ and stick them together via Sun-Ze (and Euclid).

For example, how would we get from the square root $b = 3$ of $a = 2$ mod 7 to a square root of $a = 2$ modulo 7^2 or modulo 7^3, supposing that such existed at all?

The method is due to Hensel, refered to as *Hensel's lemma.*

Strangely, this is very closely related to the Newton-Raphson method for numerical solution of equations $f(x) = 0$ in the real numbers. This method is also known as *sliding down the tangent*, and is a rare example of an algorithm that is *robust* in the sense that it is self-correcting in the face of computational errors.

The Newton-Raphson method says to find a root of $f(x) = 0$ make a first guess x_o, and then put

$$x_1 = x_o - \frac{f(x_o)}{f'(x_o)}$$

where f' is the usual derivative. Repeat as necessary:

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

This approximates the graph of $f(x)$ by the *tangent line* at x_o, and taking the intersection of the tangent line with the x-axis.

To solve $x^2 = 2$ for real x, let $f(x) = x^2 - 2$, $f'(x) = 2x$, guess $x_o = 1$, and

$$x_1 = x_o - \frac{f(x_o)}{f'(x_o)} = 1 - \frac{1^2 - 2}{2 \cdot 1} = \frac{3}{2}$$

$$x_2 = x_1 - \frac{f(x_1)}{f'(x_1)} = \frac{3}{2} - \frac{\left(\frac{3}{2}\right)^2 - 2}{2 \cdot \frac{3}{2}} = \frac{17}{12}$$

$$x_3 = x_2 - \frac{f(x_2)}{f'(x_2)} = \frac{3}{2} - \frac{\left(\frac{3}{2}\right)^2 - 2}{2 \cdot \frac{3}{2}} \approx 1.417$$

$$x_4 = x_3 - \frac{f(x_3)}{f'(x_3)} \approx 1.4142157$$

$$x_5 = x_4 - \frac{f(x_4)}{f'(x_4)} \approx 1.41421356374$$

$$x_6 = x_5 - \frac{f(x_5)}{f'(x_5)} \approx 1.414213562373$$

Hensel's Lemma says that the same process will work to get roots of equations modulo higher and higher powers of a prime. *It might be surprising that Taylor expansions and derivatives have any bearing on computations modulo p^2.*

A brute-force version of Hensel's lemma: Given that $3^2 = 2 \bmod 7$, find a square root b of 2 modulo 7^2.

Imagine that $b = 3 + 7t$ for some t, that is, by *adjusting the initial square root* 3 only by a multiple of 7. See what this requires of t

$$(3 + 7t)^2 = 2 \bmod 7^2$$

Simplify

$$9 + 42t + 49t^2 = 2 \bmod 7^2$$

Happily, the t^2 term is 0 modulo 7^2, giving a *linear* equation

$$9 + 42t = 2 \bmod 7^2$$

This linearization is not a coincidence!

The linear equation $9 + 42t = 2 \bmod 7^2$ simplifies to

$$42t + 7 = 0 \bmod 7^2$$

which says $7^2 | 7 \cdot (6t + 1)$ or simply $7|(6t+1)$, so

$$6t = -1 \bmod 7$$

We would like to multiply through by $6^{-1} \bmod 7$, which (by brute force or by extended Euclid) is 6. Thus $t = 1$.

That is, $3 + 7t = 3 + 1 \cdot 7 = 10$ should be a square root of 2 modulo 7^2. Yes,

$$10^2 = 100 = 2 \bmod 49$$

Continue this example: Modulo 7^3, try $10 + 7^2 t$ as square root, adjusting the square root mod 7^2 (namely 10) by a multiple of 7^2. Then solve for t in

$$(10 + 49t)^2 = 2 \bmod 7^3$$

Expand

$$100 + 980t + 7^4 t^2 = 2 \bmod 7^3$$

The t^2 term is 0 modulo 7^3, so this *linearizes* to

$$\begin{gathered} 100 + 980t = 2 \bmod 7^3 \\ 98 + 980t = 0 \bmod 7^3 \\ 2 + 20t = 0 \bmod 7 \\ 2 - t = 0 \bmod 7 \\ t = 2 \bmod 7 \end{gathered}$$

Thus, $10 + 7^2 t = 10 + 7^2 \cdot 2 = 108$ should be a square root of 2 mod 7^3. Indeed,

$$108^2 = 11664 = 2 \bmod 343$$

This can be systematized:

Theorem: (Hensel) Let $f(x)$ be a monic polynomial with integer coefficients. Let $f'(x)$ be the derivative of f. Let p be a prime. Let x_o be an integer such that $f(x_o) = 0 \bmod p$. Suppose that $f'(x_o) \neq 0 \bmod p$. Let $f'(x_o)^{-1} \bmod p$ be a multiplicative inverse of $f'(x_o) \bmod p$. Then

$$x_1 = x_o - f(x_o) \cdot f'(x_o)^{-1} \bmod p^2$$

is a solution of $f(x) = 0 \bmod p^2$. Similarly

$$x_2 = x_1 - f(x_1) \cdot f'(x_o)^{-1} \bmod p^3$$

is a solution of $f(x) = 0 \bmod p^3$ and

$$x_3 = x_2 - f(x_2) \cdot f'(x_o)^{-1} \bmod p^4$$

is a solution mod p^4. Etc.

Notice that the only inverse needed is $f'(x_o)^{-1} \bmod p$*, not mod* p^2 *and not* $f'(x_1)^{-1}$*, etc. Just* $f'(x_o)^{-1}$.

Example: Given that 2 is a fifth root of 3 modulo 29, find a fifth root of 3 modulo 29^2.

Note that 29 is prime (trial division). Let $f(x) = x^5 - 3$, so $f'(x) = 5x^4$. Let $x_o = 2$. Hensel's Lemma gives the next approximation (mod 29^2)

$$x_1 = x_o - f(x_o) \cdot f'(x_o)^{-1} \bmod 29^2$$

where $f'(x_o)^{-1}$ is the multiplicative inverse mod 29 (not mod 29^2)

$$f'(x_o)^{-1} = (5 \cdot 2^4)^{-1} = 80^{-1} = 4 \bmod 29$$

Thus, a fifth root of 3 mod 29^2 is

$$x_1 = 2 - (2^5 - 3) \cdot 4 = -114 = \boxed{727} \bmod 29^2$$

To get from the fifth root 727 of 3 modulo 29^2 to a fifth root of 3 mod 29^3, repeat: still with $f(x) = x^5 - 3$,

$$x_2 = x_1 - f(x_1) \cdot f'(x_o)^{-1} \bmod 29^3$$

Again, note that the inverse of the value of the derivative is just the inverse mod 29 which we computed (namely, 4), not mod 29^2 nor 29^3. Thus, the next approximation is a fifth root of 3 modulo 29^3

$$x_2 = 727 - (727^5 - 3) \cdot 4 = \boxed{12501} \bmod 29^3$$

Continuing in this manner gives a fifth root of 3 modulo any power of 29.

Note that the new mod 29^{t+1} solution is congruent to the previous (mod 29^t) solution modulo 29^t.