Supplementary Notes for Post-Quantum Cryptography Video

November 4, 2025

A: Existence of Magic Powers

Proof. Something I state without proof in the video is the well-known fact that every positive integer N has a "magic power" r. This has the property that $x^r \equiv 1 \bmod N$ for every x coprime with N. To get there, we need to first establish that there exists an integer y such that $xy \equiv 1 \bmod N$.

Consider Bezout's Identity, which tells us that:

(i) All integer combinations $ax + bN$ are multiples of the greatest common divisor of x and N.

(ii) There exists integers a and b such that $ax+bN = d$, where d is the greatest common divisor of x and N.

If you want a more thorough dive into that, I explored it in my DVD Screensaver video. Applying this to the case where x and N are coprime (and so their greatest common divisor is 1) we know by Bezout (ii) that there exist integers y and b with $xy + bN = 1$. In other words, $xy = 1 - bN$ and so $xy \equiv 1 \bmod N$.

Now we've established that, let's start taking powers of x, modulo N. Because there are a finite number of residues modulo N (i.e. $0 \leq (x^a \bmod N) < N$), if we continue taking powers, repetition is inevitable. So, let $x^b \equiv x^a \bmod N$ where $b > a$. This implies that $x^b y \equiv x^a y \bmod N$, and we can use this to "scrape away" one copy of x:

$$\begin{aligned} & x^b \equiv x^a \bmod N \\ \implies & x^b y \equiv x^a y \bmod N \\ \implies & x^{b-1}(xy) \equiv x^{a-1}(xy) \bmod N \\ \implies & x^{b-1} \equiv x^{a-1} \bmod N \end{aligned}$$

We can repeat this up to a total of a times, therefore

$$x^{b-a} \equiv x^{a-a} \bmod N \equiv 1 \bmod N$$

Thus we have shown that there exists a power of x which is congruent to 1, modulo N. ■

B: Magic powers are only for x and N coprime

So, if the magic power of N is r, then $x^r \equiv 1 \bmod N$, but only for an x which is coprime with N. What goes wrong with x and N are not coprime? I encourage you to do some experiments and observe what happens. For example, taking powers of 2 modulo 10 results in the repeating pattern of $2, 4, 8, 6, 2, 4, 6, 8 \ldots$. It comes down to Bezout (i).

Proof. Suppose $x \neq 1$ and N are not coprime. That means they have a greatest common divisor $d \neq 1$. Now suppose for contradiction that $x^t \equiv 1 \bmod N$, for $t > 0$. Well, that means that we have found a such that $ax \equiv 1 \bmod N$. (Here, $a = x^{t-1}$ but we don't care what a is, just that it exists.) This now means that $ax = 1 + bN$ for some integer b, and therefore $ax - bN = 1$. But Bezout (i) tells us that all such integer combinations are multiples of d, a contradiction. ■

If you're wondering what goes wrong with the proof of **A** when we try to apply it to this case, it's when we bring in y to scrape away those powers of x. As we've just seen, that y doesn't exist when x and N share a factor!

C: Fermat's Little Theorem

As a reminder, this states that if p is prime, then $x^p \equiv x \bmod p$ where x and p are coprime. There are many proofs, and I think the most accessible one "from first principles" is the inductive proof found here. You know me though, I'm a group theorist, so let me show you a group-theoretic approach. The only thing I'll use without proof is Lagrange's Theorem: If H is a subgroup of a finite group G, then the order of H divides the order of G.

Proof. Equip the set of integers $\{1, \ldots, p-1\}$ with the operation of multiplication modulo p. I claim that this is a group. It is closed, as taking numbers modulo p reduces them to a number in $\{0, \ldots, p-1\}$, but it isn't possible that $xy \equiv 0 \bmod p$ for $x, y \in \{1, \ldots, p-1\}$ – that would suggest that $xy = kp$ for some integer k, and so p divides x or y which is absurd. Multiplication is associative, and 1 is the identity. As for inverses, we showed earlier that if x and N are coprime, then there is an integer y with $xy \equiv 1 \bmod N$. Since p is prime, then all $x \in \{1, \ldots, p-1\}$ are coprime with p. So, there is an integer y with $xy \equiv 1 \bmod p$. We just need to show that such a y can be selected from the set $\{1, \ldots, p-1\}$. Let y_0 be *some* integer with $xy \equiv 1 \bmod p$, and now subtract copies of p until we have a number in the desired range: $y = y_0 - kp \in \{1, \ldots, p-1\}$. Now: $xy = xy_0 - xkp \equiv 1 - 0 \bmod p$. Hence every element has an inverse, and $\{1, \ldots, p-1\}$ is a group.

Now, let $x \in \{1, \ldots, p-1\}$ and let its order be r (that is, the smallest positive integer with $x^r = 1$ which in this context means $x^r \equiv 1 \bmod p$) and consider the set of powers of x, i.e. $\{1, x, x^2, x^3, \ldots, x^{r-1}\}$. This is a subgroup of $\{1, \ldots, p-1\}$. I'll leave the demonstration of this as an exercise (huh, so I guess Lagrange's Theorem isn't the *only* result I'm stating without proof). But as a subgroup, its order, r, must divide the order of $\{1,\ldots,p-1\} = p-1$. This means $kr = p-1$ for some integer k. The rest of the proof writes itself:

$$x^p = x \cdot x^{p-1} = x \cdot x^{kr} = x \cdot (x^r)^k \equiv x \cdot 1^k \bmod p.$$

■

D: The magic power of semiprimes

The final bit I gloss over is the fact that if $N = pq$ for primes p and q, then the magic power of N is calculated by taking the lowest common multiple of $p-1$ and $q-1$. For more details on this, the search term you are looking for is the Carmichael Function, which returns the "magic power" and has an associated formula.

Proof. To prove this, recall that the magic power of a prime p is $p-1$, as we see from Fermat's Little Theorem. We'll go one step further here and say that this is actually the minimal magic power. To be clear, this does not directly follow from Fermat's Little Theorem, which establishes that $x^{p-1} \equiv 1 \bmod p$ for any x coprime with p. However, this doesn't preclude the possibility that for a particular p there is a smaller number $r < p-1$ which just so happens to have the property that $x^r \equiv 1 \bmod p$ for every x coprime with p. As it turns out, this is impossible. One way to prove this is by showing that $\{1,\ldots,p-1\}$ is a cyclic group (that is, there exists $g \in \{1,\ldots,p-1\}$ such that g has order $p-1$). It's not so easy to show this, and I won't do so here, but I will link to this amazing article compiling a great many proofs.

So, let's take it as a fact that $p-1$ is the minimal magic power of p. From here, we first show that whatever the magic power of pq is, it must be a multiple of $p-1$. Indeed, suppose r is the minimal magic power of pq, and divide it by $p-1$, obtaining $r = a(p-1)+b$ where $0 \leq b < p-1$. Now, first of all, note that $x^r \equiv 1 \bmod p$. This is because given $x^r \equiv 1 \bmod pq$, we have $x^r = kpq + 1 = (kq)p + 1 \equiv 1 \bmod p$. So now, we have:

$$1 \bmod p \equiv x^r = x^{a(p-1)+b} = (x^{p-1})^a \cdot x^b \equiv 1^a x^b$$

But now $x^b \equiv 1 \bmod p$ with $b < p-1$ forces us to conclude that $b = 0$, seeing as $p-1$ is the minimal integer with this property. Hence $r = a(p-1)$, and r is a multiple of $p-1$, as claimed.

As you might have predicted, all the same arguments apply to q, so we conclude that r must be a multiple of both $p-1$ and $q-1$. Their lowest common multiple is the smallest such integer, which essentially provides a lower bound for the magic power of pq. It remains to be shown that the LCM of $p-1$ and $q-1$ actually has the magic power property, but this is straightforward. Let m be the LCM of $p-1$ and $q-1$, and let x and pq be coprime. Because m is a multiple of $p-1$, suppose $m = (p-1)k$ and:

$$x^m = x^{(p-1)k} = (x^{p-1})^k \equiv 1^k \bmod p$$

A similar argument establishes that $x^m \equiv 1 \bmod q$. Therefore, $x^m = ap + 1 = bq + 1$ for integers a and b. In other words, $x^m - 1 = ap = bq$. But because p and q are prime, both p and q must divide $x^m - 1$. Also, because p and q are prime, pq must divide $x^m - 1$. Say, $cpq = x^m - 1$ and so $x^m = c(pq) + 1$, which yields $x^m \equiv 1 \bmod pq$, as required. ■