§7. Miscellany—We’ll now discuss a few pieces of ‘early modern’ mathematics that I think are rather cool and which build on the same body of theory we’ve been working on all semester. Here’s a little fact to get us started.

**Proposition 1.** Suppose that $p$ is a prime number, and $[a]_p \in \mathbb{Z}/p$. Then

$$[(p - 1)!]_p = \begin{cases} -[a]_p^{(p-1)/2} & \text{if } a \text{ is a square mod } p \\ [a]_p^{(p-1)/2} & \text{(otherwise)} \end{cases}$$

*Proof.* We can group all the nonzero numbers mod $p$ into pairs $\{[x]_p, [y]_p\}$, where $[xy]_p = [a]_p$. Everything pairs up nicely, except that if $x$ has the property that $[x^2]_p = [a]_p$, then $x$ will pair with itself. We then have two cases.

If $a$ is not a square mod $p$, then everything pairs up nicely. There are $p - 1$ numbers to pair up, and so we get $(p - 1)/2$ pairs. When we multiply all the pairs together, we get $[a^{(p-1)/2}]_p$, since each pair multiplies to give $[a]_p$. But doing this, we’ve also multiplied together all $p - 1$ numbers mod $p$, so made $[(p - 1)!]_p$. Thus

$$[(p - 1)!]_p = [a]_p^{(p-1)/2} \quad \text{if } a \text{ is a not a square mod } p$$

If $a$ is a square mod $p$, and $[x]_p$ is one number that squares to $[a]_p$, then $[-x]_p$ is the only other such number. (We can factorize the polynomial $T^2 - [a]_p$ over the field $\mathbb{Z}/p$ as $(T - [x]_p)(T + [x]_p)$; so using the domain property any solution must either satisfy $T - [x]_p = 0$ or $T + [x]_p = 0$. Then

$$[(p - 1)!]_p = [a]_p^{(p-3)/2}[x]_p[-x]_p = -[a]_p^{(p-1)/2} \quad \text{if } a \text{ is a not a square mod } p$$

Combining these, we’re done. \qed

Now, 1 is always a square mod $p$, so we deduce ‘Wilson’s theorem’:

**Corollary 2** (Bhaskara c700CE, Ibn al-Haytham c1000CE). We have that $[(p - 1)!]_p = [-1]_p$.

**Corollary 3.** Let $p$ be an odd prime. We have that $-1$ is a square mod $p$ just if $[p]_4 = 1$.

*Proof.* Plugging Wilson’s theorem into Prop 1, and putting $a = -1$, and spotting that we can forget about the $[-]_p$ because everything either 1 or -1, we see:

$$-1 = \begin{cases} -(-1)^{(p-1)/2} & \text{if } a \text{ is a square mod } p \\ (-1)^{(p-1)/2} & \text{(otherwise)} \end{cases}$$

So we see that $-1$ is a square mod $p$ iff $(-1)^{(p-1)/2}$ is 1, which is true iff $(p - 1)/2$ is even, i.e. iff $p$ is 1 mod 4. \qed

**Proposition 4.** Suppose $p$ is a prime, and $[p]_4 = [3]_4$; and that $p|n$ but $p^2 \not| n$. Then $n$ cannot be written as a sum of two squares.

*Proof.* If so, we would have $n = a^2 + b^2$. I first claim that we know that at least one of $a$ and $b$ is not divisible by $p$. For otherwise, the RHS is divisible by $p^2$, a contradiction. Let’s suppose $a$ isn’t divisible, so $[a]_p \neq [0]_p$.

We when notice that we have $[a]_p^2 + [b]_p^2 = [0]_p$. We know that there’s a number such that $[t]_p[a]_p = [1]_p$, since $\mathbb{Z}/p$ is a field. Then $[1]_p + [bt]_p^2 = 0$, or $[bt]_p^2 = [-1]_p$, which contradicts the corollary. \qed