Note: These notes are based on online material including examples from Wikipedia (see references below)

1 Problem and Model

1.1 Multiplicative groups

The *multiplicative group* $\mathbb{Z}_q^*$ is the set of all integers that are coprime (relatively prime) to q in the set $\{1, \ldots, n-1\}$ along with the multiplication operation modulo q

For example, $\mathbb{Z}_7^*$ is the set $\{1, 2, 3, 4, 5, 6\}$, where multiplication occurs modulo q. What does this mean? It means that in the group $\mathbb{Z}_7^*$, $4 \cdot 5 = 6$, since $(4 \cdot 5 \bmod 7) = (20 \bmod 7) = 6$.

1.2 Fermat's Little Theorem

The following inductive proof is due to Euler, by way of Wikipedia. First we need a helper lemma.

Lemma 1. *For any integers x and y and for any prime p,*

$$(x+y)^p \equiv x^p + y^p \pmod{p}$$

Proof: Recall from the binomial theorem that

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$$

where

$$\binom{n}{i} = \frac{n!}{i!(n-i)!}$$

Now consider the binomial coefficient when p is prime and $0 < i < p$:

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

The numerator has a factor p, the denominator has no factor of p, and the coefficient is an integer. So, the coefficient must include a factor of p. Thus, for all $0 < i < p$,

$$\binom{p}{i} \equiv 0 \pmod{p}$$

So for any prime p:

$$\begin{aligned}(x+y)^p &\equiv \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i \pmod{p} \\ &\equiv \binom{p}{0} x^p + \binom{p}{p} y^p \pmod{p} \\ &\equiv x^p + y^p \pmod{p}\end{aligned}$$

□

Now, for the main (little) course: Fermat's Little Theorem.

Theorem 1. *For every prime p and integer a,*

$$a^p \equiv a \pmod{p}$$

Proof: By induction on a.
BC: $0^p \equiv 0 \pmod{p}$
IH: Assume $(a-1)^p \equiv (a-1) \pmod{p}$
IS: Using the fact that $a = (a-1)+1$, we have the following mod p

$$\begin{aligned} ((a-1)+1)^p &\equiv (a-1)^p + 1^p && \text{By Lemma 1} \\ &\equiv (a-1) + 1^p && \text{By IH} \\ &\equiv a \end{aligned}$$

□

1.2.1 FLT shows that $\mathbb{Z}_p^*$ is a group

Fermat's Little theorem (FLT) shows that $\mathbb{Z}_p^*$, by showing that every element has an inverse.

In particular, consider any element a in $\mathbb{Z}_p^*$. By FLT, $a \cdot a^{p-2} \equiv a^{p-1} \equiv 1$. Hence, a^{p-2} is the inverse of a.

1.3 The group $\mathbb{Z}_p^*$ is cyclic

A group G of size n is called *cyclic* if there exists some element $g \in G$ such that for all $g' \in G$, $g' = g^i$ for some integer $i \in [0, n-1]$.

For a group G and element $x \in G$, let *ord(x)* be the smallest positive integer i such that $x^i = 1$.

In a finite group, every element has finite order. Can you see why??? Hint: remember that every element has an inverse.

Lemma 2. *The group $\mathbb{Z}_p^*$ is cyclic.*

Proof: Let $\ell = lcm(ord(1), ord(2), \ldots, ord(p-1))$ (recall that lcm is the least common multiple, so $lcm(4,6) = 12$).) Then, for all $a \in \mathbb{Z}_p^*$, since $ord(a)|\ell$, we've got:

$$a^\ell \equiv 1$$

Now consider the degree ℓ polynomial $x^\ell - 1$ in $\mathbb{Z}_p$. By the above argument, it must have at least p roots, since $a^\ell - 1 = 0$ for all $a \in \mathbb{Z}_p^*$. Since the degree of a polynomial must be as large as the number of roots, $\ell \geq p-1$.

Next, note that for any pair of elements a and b, there is an element that has order $lcm(a,b)$ – this is just the element $a \cdot b$. Applying this repeatedly, it means there must be an element g of order ℓ. Hence $\ell \leq p-1$. Combining with the fact that $\ell \geq p-1$, shows that there must be an element of order $p-1$. □

2 Interactive proof of Knowledge

With all of the above lemmas in hand, let's devise an interactive proof of knowledge

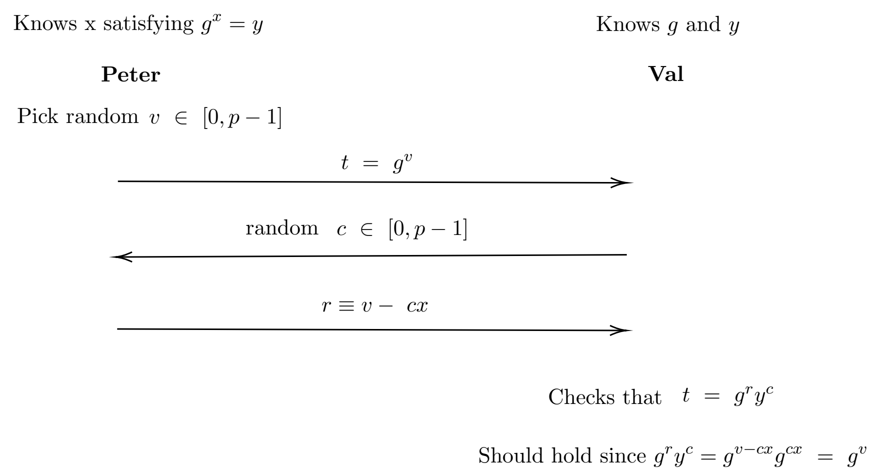

Figure 1. Fiat-Shamir Interactive

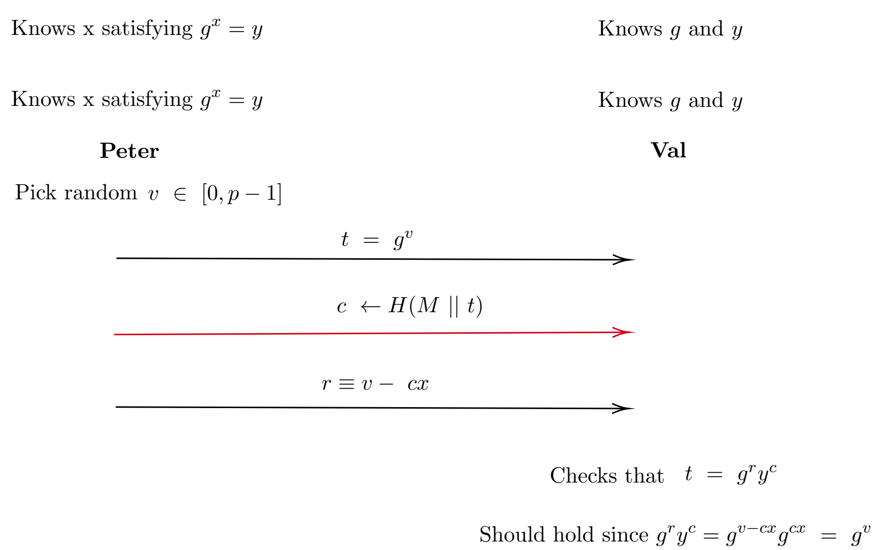

Figure 2. Fiat-Shamir Digital Signature. M is the messages. H is a cryptographic hash function.

3 References

Fiat-Shamir https://www.math.auckland.ac.nz/~sgal018/crypto-book/ch22.pdf

Fermat's Little Theorem: https://en.wikipedia.org/wiki/Proofs_of_Fermat%27s_little_theorem

Proof that Z_p^* is cyclic: https://math.stackexchange.com/questions/1240353/cyclic-group-zp