MA-224 - WEEK 44
APPLICATIONS OF LAGRANGE'S THEOREM

SVERRE LUNØE–NIELSEN

Contents

1. Introduction

We will discuss topics from [1, §16.10]. Recall from last week:

Theorem 1.1 (Lagrange's theorem)**.** *Let G be a finite group, and let $H \subset G$ be a subgroup. Then $|G| = |H| \cdot [G : H]$.*

From this fundamental fact, we get various interesting applications. We first look at a classical consequences in number theory, before we see how this makes the RSA encryption scheme work.

2. Euler's theorem

Euler's theorem is about modular multiplication. Recall from last week the multiplicative group of integers mod (n)

$$P_n = \{k \in \mathbb{Z} \mid 1 \leq k < n,\ \gcd(k, n) = 1\}$$

with group operation given by integer multiplication modulo n.

The following is a consequence of Lagrange's theorem:

Corollary 2.1. *Let G be a finite group of order $n = |G|$ and with neutral element $e \in G$. Then $g^n = e$ for all $g \in G$.*

Proof. Let k be the order of the cyclic subgroup $H = \langle g \rangle \subset G$. Then since H is cyclic, we know that the order of its generator g is the same as k. Lagrange's theorem says that $n = k \cdot [G : \langle a \rangle]$, which means that

$$g^n = g^{k \cdot [G:\langle a \rangle]} = (g^k)^{[G:\langle a \rangle]} = e^{[G:\langle a \rangle]} = e\,.$$

□

Date: November 2, 2022.

Definition 2.2 (Euler's totient function)**.** *Let $n > 0$ be a natural number. Euler's totient function ϕ is defined as*

$$\phi(n) = |P_n|$$

i.e. as the number of positive integers less than n which are coprime to n.

Lemma 2.3. *Let p be a prime number. Then $\phi(p) = p - 1$.*

Proof. Every positive integer less than p is coprime to p since p is a prime number. □

Lemma 2.4. *Let p and q be prime numbers. Then $\phi(pq) = \phi(p)\phi(q)$.*

Proof. The proof is an exercise left to the reader. □

Theorem 2.5 (Euler's theorem)**.** *Let a and n be coprime natural numbers. Then*

$$a^{\phi(n)} = 1 \mod (n)$$

Proof. This is a reformulation of Corollary 2.1 when $G = P_n$. □

Corollary 2.6 (Fermat's little theorem)**.** *Let p be a prime. Then for any integer $1 \leq a < p$,*

$$a^{p-1} = 1 \mod (p)$$

Proof. Since p is prime, any number $1 \leq a < p$ is an element of P_p, and Lagrange's theorem implies that $a^{\phi(p)} = 1 \mod (p)$. But then the result follows by 2.3. □

Fermat's little theorem can be used as a test for non-primality:

Example 2.7 To prove that 527 is not a prime, we choose any an integer a and compute $a^{527-1} \mod (527)$. If the answer is different from 1, then 527 isn't a prime number. E.g. if $a = 2$, then $2^{526} = 64 \neq 1 \mod (527)$, and therefore 527 is not a prime number.

The same thing happens when $n = 1935$, when we choose $a = 2$: Since $a^{1934} = 4 \mod (1935)$ and so we can conclude that 1935 is not a prime number.

We chose the base number $a = 2$ because it was small and therefore easier to compute with. But sometimes we need to work with other base numbers to find a conclusion. As an example we will see that 1105 is not a prime. First we try with $a = 2$, but then we get $2^{1104} = 1 \mod (1105)$ so no conclusion can be drawn. We get the same result for $a = 3$ and 4 too, but letting $a = 5$ results in $5^{1104} = 885 \mod (1105)$, and the conclusion is therefore that 1105 isn't a prime number.

3. The RSA encryption scheme

Choose prime numbers p and q, and let $n = pq$ be their product. Then choose numbers $x, y < \phi(n)$ such that

$$xy = 1 \mod (\phi(n)). \tag{1}$$

We claim that $x, y \in P_{\phi(n)}$: Let $r = \phi(n)$. If $xy = 1 \mod (r)$, then $xy = 1 + kr$ for some integer k. This implies that xy is not divisable by any of the prime factors of r. Therefore, $\gcd(xy, r) = 1$, and from this it follows that $\gcd(x, r) = \gcd(y, r) = 1$. In other words, x and y belong to the set P_r.

We are now ready to encrypt! Let $0 \leq m < n$ be our message. Then the enrypted message is defined to be

$$e(m) = m^x \mod (n).$$

Decryption works in the same way, using the integer y as exponent. For an encrypted message M, recover the decrypted plain text message by

$$d(M) = M^y \mod (n).$$

The reason this works is because e and d are inverse functions. To see this, assume that $\gcd(m, n) = 1$. Then

$$\begin{aligned} d(e(m)) &= (m^x)^y \\ &= m^{xy} \\ &= m^{1+k\phi(n)} \\ &= m \cdot (m^{\phi(n)})^k \\ &= m \cdot 1^k = m \mod (n). \end{aligned}$$

The equality $m^{\phi(n)} = 1$ is Euler's theorem.

There is essentially one more case to check, namely $\gcd(m, n) = p$: In this case we use the fact that two integers a and b are equal modulo n if and only if $a = b \mod (p)$ and $a = b \mod (q)$ at the same time. (proof: Corollary of $p \mid x$ and $q \mid x \Leftrightarrow pq \mid x$.) Thus, if $p \mid m$ then

$$d(e(m)) = m^{xy} = 0 = m \mod (p).$$

Lastly, we want to show that $d(e(m)) = m \mod (q)$. To do this, we need the identity $\phi(pq) = \phi(p)\phi(q)$ from Lemma 2.4. We then get

$$m^{\phi(n)} = (m^{\phi(q)})^{\phi(p)} = 1^{\phi(m)} = 1 \mod (q).$$

The middle equivalence uses that $\gcd(m, q) = 1$ together with Euler's theorem. Finally,

$$d(e(m)) = m \cdot (m^{\phi(n)})^k = m \cdot 1^k = m \mod (q).$$

3.1. **Private and public keys.** In public key cryptography using the RSA encryption scheme, one talks about public and private keys. In the above setting, the public key concists of the pair (n, x), and the private key (n, y).

This way, anyone can encrypt messages, but only the owner of the private key can decrypt messages since it requires the knowledge of y.

References

[1] Ralph P. Grimaldi, *Discrete and combinatorial mathematics: an applied introduction.*, Pearson Education, 2013.

Email address: sverre.lunoe-nielsen@uia.no