15-251: Great Theoretical Ideas In Computer Science

Recitation 13 Solutions

Euler is Even

Prove that for any $n > 2$, $\phi(n)$ is even.

Suppose k is relatively prime to n, so gcd(k,n) $= 1$. We'll first show that gcd($n-k$, n) $= 1$.

Since gcd(k,n) $= 1$, we know by Euler that there exist x, y so that $kx + ny = 1$. Thus we have $1 = kx + ny = kx + ny - nx + nx = (k-n)x + n(x+y) = (n-k)(-x) + n(x+y)$. Since x, y integers, so are $x + y$ and $-x$.
Thus we have gcd($n-k$, n) | 1, so gcd($n-k$, n) $= 1$.

Now, we use this to pair off elements in Z_n^*.
First note that $\frac{n}{2} \notin Z_n^*$, since either n is odd or since $n > 2$, gcd($\frac{n}{2}$, n) $= \frac{n}{2} > 1$.
Now, for each $k \in Z_n^*$, $n-k \in Z_n^*$, and $n-k \neq k$. Thus $\phi(n) = |Z_n^*|$ is even for $n > 2$.

RSA Practice

In lecture, we saw how RSA encryption is used. There are many important quantitites used in this algorithm:

- p, q: Two very large prime numbers.
- n: $n = pq$ is part of the public key
- $\phi(n)$: Since p, q prime, $\phi(n) = (p-1)(q-1)$
- e: e, also part of the public key, is some member of $\mathbb{Z}^*_{\phi(n)}$
- d: d, the private key, is the inverse of e in $\mathbb{Z}^*_{\phi(n)}$, i.e. $ed \cong_{\phi(n)} 1$
- m: This is the message that will be sent

Let $p = 17$, $q = 7$, $e = 11$

(a) Use the extended Euclidian Algorithm to find d.

First, we must find $\phi(n)$. $\phi(n) = (p-1)(q-1) = 16 * 6 = 96$. We must find d such that $11d \equiv_{96} 1$. We have:

$$\begin{aligned} 96 &= 11 \times 8 + 8 \\ 11 &= 8 \times 1 + 3 \\ 8 &= 3 \times 2 + 2 \\ 3 &= 2 \times 1 + 1 \end{aligned}$$

Now we work backwards:

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (8 - 3 \times 2) = 3 \times 3 - 8 \\ &= (11 - 8) \times 3 - 8 = (11 \times 3) - (8 \times 4) \\ &= (11 \times 3) - ((96 - 11 \times 8) \times 4) = (11 \times 35) - (96 \times 4) \end{aligned}$$

Thus, $d = 35$.

(b) Encrypt the message 3

First, we find n which is pq which is 119. We need to find 3^{11} mod 119. This is

$$\begin{aligned} 3^{11} &\equiv_{119} 3 * 3^5 * 3^5 \\ &\equiv_{119} 3 * 243 * 243 \\ &\equiv_{119} 3 * 5 * 5 \\ &\equiv_{119} 75 \end{aligned}$$

(c) Decrypt the message 2

We need to find 2^{35} mod 119. This is

$$\begin{aligned} 2^{35} &\equiv_{119} 2^{7^5} \\ &\equiv_{119} 128^5 \\ &\equiv_{119} 9^5 \\ &\equiv_{119} 3^5 * 3^5 \\ &\equiv_{119} 243 * 243 \\ &\equiv_{119} 5 * 5 \\ &\equiv_{119} 25 \end{aligned}$$

Groups

Define $\bullet : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ as follows: For all $x, y \in \mathbb{N}$,
$x \bullet 3 = x$

$3 \bullet y = y$
$x \bullet y = x + y$ if both $x, y \neq 3$

Is $(\mathbb{N}, \bullet)$ a group?
For each of the four required properties of a group, prove or disprove that they hold for $(\mathbb{N}, \bullet)$.

Closure:
For all $x, y \in \mathbb{N}$, x, y, and $x + y$ are also in $\mathbb{N}$. Thus closure is satisfied.

Associativity:
Not satisfied: $(1 \bullet 2) \bullet 4 = 3 \bullet 4 = 4$, but $1 \bullet (2 \bullet 4) = 1 \bullet 6 = 7$.

Identity:
This is satisfied, because 3 is an identity. $\forall x \in \mathbb{N}$, $x \bullet 3 = 3 \bullet x = x$.

Inverses:
Not satisfied: Only 1, 2, and 3 have inverses. 0 has no inverse because $0 \bullet x$ is x for $x \neq 3$ and 0 if $x = 3$. Thus there is no x such that $0 \bullet x = 3$.

Orders

Let G be an abelian group with operation $\cdot$.
Let $x, y \in G$ have $|x| = m$ and $|y| = n$ with $\gcd(m, n) = 1$. Show that $|x \cdot y| = mn$.

We need to show that mn is the least k such that $(x \cdot y)^k = e$.

We have $(x \cdot y)^{mn} = x^{mn} \cdot y^{mn}$ because G is abelian. Furthermore, $x^{mn} = (x^m)^n = e^n = e$ and $y^{mn} = (y^n)^m = e^m = e$, so $(x \cdot y)^{mn} = e$.

Now, suppose $(x \cdot y)^k = e$. Then $e = (x \cdot y)^{mk} = x^{mk} \cdot y^{mk} = y^{mk}$, so $n | mk$. Similarly, $e = (x \cdot y)^{nk} = x^{nk} \cdot y^{nk} = x^{nk}$, so $m | nk$.

Thus $mn | m^2 k$ and $mn | n^2 k$, so $mn | \gcd(m^2 k, n^2 k) = k$. Therefore $mn \leq k$, so $|x \cdot y| = mn$.