Homework 5

(1) For each of the following prime p, find a generator of $\mathbb{Z}_p^*$.

(a) $p = 17$

(b) $p = 29$

(c) $p = 31$

(2) If you pick any integer from $\mathbb{Z}_p^*$ randomly: What's the probability that it is a generator of $\mathbb{Z}_p^*$?

(a) $p = 17$

(b) $p = 29$

(c) $p = 31$

Homework 5

(1) For each of the following prime P, find a generator of $\mathbb{Z}_p^*$.

(a) $p = 17$

$ord(g) = 16 = 2^4$

$\forall h \in \mathbb{Z}_p^*$, $ord(h) \mid |\mathbb{Z}_p^*| = 16 = 2^4$

$ord(h) = 2^i$ for some i

Take $h \in \mathbb{Z}_p^*$, if $h^{2^3} \neq 1 \mod 16$

then $ord(h) = 2^4$

hence, h is a generator

(b) $p = 29$

(c) $p = 31$

(2) If you pick any integer from $\mathbb{Z}_p^*$ randomly: What's the probability that it is a generator of $\mathbb{Z}_p^*$?

(a) $p = 17$

(b) $p = 29$

(c) $p = 31$

$$\frac{\#\text{ of generators}}{\text{size of group}} = \frac{\varphi(p-1)}{p-1}$$

If g is a generator then g^i is also a generator if i is coprime with $p-1$.

1 b)

$p = 29$

$p-1 = 28 = 2^2 \cdot 7$

$\forall\, h \in \mathbb{Z}_p^{\times}$, $\operatorname{ord}(h) = 2^i \cdot 7^j$ $\quad 0 \le i \le 2$, $0 \le j \le 1$

If $h^{2^2} \neq 1$ and $h^{2 \cdot 7} \neq 1$, then the $\operatorname{ord}(h) = 2^2 \cdot 7$.

If $h^{2^2} \neq 1$, what could be the order of h?

$7,\ 2 \cdot 7,\ 2^2 \cdot 7$

Hence, if in addition, $h^{2 \cdot 7} \neq 1$, then the only order of h is $2^2 \cdot 7$.

To find a generator of a group of order n.

$n = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$

$n_i = \dfrac{n}{p_i}$

Pick $h \in G$. If $h^{n_i} \neq 1$ for all i

then h is a generator.

2) $\dfrac{\varphi(p-1)}{p-1}$

(a) $p = 17$, probability is $\dfrac{\varphi(16)}{16} = \dfrac{\varphi(2^4)}{16} = \dfrac{1}{2}$

(b) $p = 29$, probability is $\dfrac{\varphi(28)}{28} = \dfrac{\varphi(2^2)\varphi(7)}{2^2 \cdot 7}$

$= \dfrac{2 \cdot 6}{4 \cdot 7}$

$= 3/7$

generator $g \in G$ is such that

$\langle g \rangle = \{ g^i, i \in \mathbb{Z} \} = G$

$\forall h \in G$, $h = g^i$ for some i

If $g=3$ is a generator,

then all elements in G is 3^i

for some i

---

(3) Let $g \in G$ be a group element.

Prove that $\operatorname{ord}(g^i) = \dfrac{\operatorname{ord}(g)}{\gcd(i, \operatorname{ord}(g))}$

(4)

2.17. Use Shanks's babystep–giantstep method to solve the following discrete logarithm problems. (For (b) and (c), you may want to write a computer program implementing Shanks's algorithm.)

(a) $11^x = 21$ in $\mathbb{F}_{71}$.

(b) $156^x = 116$ in $\mathbb{F}_{593}$.

(c) $650^x = 2213$ in $\mathbb{F}_{3571}$.

(4)

modulo 71

2.17. Use Shanks's babystep–giantstep method to solve the following discrete logarithm problems. (For (b) and (c), you may want to write a computer program implementing Shanks's algorithm.)

(a) $11^x = 21$ in $\mathbb{F}_{71}$.
(b) $156^x = 116$ in $\mathbb{F}_{593}$.
(c) $650^x = 2213$ in $\mathbb{F}_{3571}$.

Recap: $x = im + j$ $\quad 0 \le i < m$, $0 \le j < m$ $\quad m = \lceil \sqrt{70} \rceil = 9$

L1: $11, 11^2, 11^3, \ldots, 11^8$ $\quad u = 11^{-9} = 7$

L2: $21, 21 \cdot 7, 21 \cdot 7^2, \ldots$ $\quad h = 21$

Find a match i, j such that $11^i = 21 \cdot 7^j$

Verify that $11^x = 21$ by performing square and multiply

(5)

2.27. Write out your own proof that the Pohlig–Hellman algorithm works in the particular case that $p-1 = q_1 \cdot q_2$ is a product of two distinct primes. This provides a good opportunity for you to understand how the proof works and to get a feel for how it was discovered.

(5)

2.27. Write out your own proof that the Pohlig–Hellman algorithm works in the particular case that $p-1 = q_1 \cdot q_2$ is a product of two distinct primes. This provides a good opportunity for you to understand how the proof works and to get a feel for how it was discovered.

Solve $g^x = h$ where $\operatorname{ord}(g) = p-1 = q_1 \cdot q_2$ in $\mathbb{Z}_p^*$

$g_1 = g^{q_2}$, $h_1 = h^{q_2}$, $\operatorname{ord}(g_1) = \operatorname{ord}(g^{q_2}) = q_1$

$g_2 = g^{q_1}$, $h_2 = h^{q_1}$, $\operatorname{ord}(g_2) = q_2$

Solve x_1 and x_2 such that

$g_1^{x_1} = h_1$

$g_2^{x_2} = h_2$

Solve x such that $x \equiv x_1 \mod q_1$
$x \equiv x_2 \mod q_2$

Since $\gcd(q_1, q_2) = 1$, there exists integers u, v such that

$$q_1 u + q_2 v = 1$$

$$x = x_1 q_2 v + x_2 q_1 u$$

Verify that $g^x = h$

$$g^x = g^{x_1 q_2 v + x_2 q_1 u} = g^{x_1 q_2 v} \cdot g^{x_2 q_1 u} = g^{q_2 x_1 v} \cdot g^{q_1 x_2 u}$$
$$= g_1^{x_1 v} \cdot g_2^{x_2 u}$$
$$= h_1^{v} \cdot h_2^{u}$$
$$= h^{q_2 v} \cdot h^{q_1 u} = h^{q_2 v + q_1 u} = h$$

(6)

3.14. We stated that the number 561 is a Carmichael number, but we never checked that $a^{561} \equiv a \pmod{561}$ for every value of a.

(a) The number 561 factors as $3 \cdot 11 \cdot 17$. First use Fermat's little theorem to prove that

$$a^{561} \equiv a \pmod{3}, \quad a^{561} \equiv a \pmod{11}, \quad \text{and} \quad a^{561} \equiv a \pmod{17}$$

for every value of a. Then explain why these three congruences imply that $a^{561} \equiv a \pmod{561}$ for every value of a.

The next six Carmichael numbers are (sequence A002997 in the OEIS):

$$\begin{array}{ll}
1105 = 5 \cdot 13 \cdot 17 & (4 \mid 1104; \quad 12 \mid 1104; \quad 16 \mid 1104) \\
1729 = 7 \cdot 13 \cdot 19 & (6 \mid 1728; \quad 12 \mid 1728; \quad 18 \mid 1728) \\
2465 = 5 \cdot 17 \cdot 29 & (4 \mid 2464; \quad 16 \mid 2464; \quad 28 \mid 2464) \\
2821 = 7 \cdot 13 \cdot 31 & (6 \mid 2820; \quad 12 \mid 2820; \quad 30 \mid 2820) \\
6601 = 7 \cdot 23 \cdot 41 & (6 \mid 6600; \quad 22 \mid 6600; \quad 40 \mid 6600) \\
8911 = 7 \cdot 19 \cdot 67 & (6 \mid 8910; \quad 18 \mid 8910; \quad 66 \mid 8910).
\end{array}$$

If n is a Carmichael number then n is a product of distinct primes.

$n = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ $\quad p_i$ are distinct primes

$\mathbb{Z}_n^{\vee} \cong \mathbb{Z}_{p_1^{e_1}}^{*} \times \mathbb{Z}_{p_2^{e_2}}^{*} \times \cdots \times \mathbb{Z}_{p_n^{e_n}}^{*}$

(6)

3.14. We stated that the number 561 is a Carmichael number, but we never checked that $a^{561} \equiv a \pmod{561}$ for every value of a.

(a) The number 561 factors as $3 \cdot 11 \cdot 17$. First use Fermat's little theorem to prove that

$$a^{561} \equiv a \pmod{3}, \quad a^{561} \equiv a \pmod{11}, \quad \text{and} \quad a^{561} \equiv a \pmod{17}$$

for every value of a. Then explain why these three congruences imply that $a^{561} \equiv a \pmod{561}$ for every value of a.

n is carmichael number if $\forall a \in [1, \ldots, n-1]$

$a^{n-1} \equiv 1 \bmod n$ and n is composite

$\simeq$ $a^n \equiv a \bmod n$

Fermat little theorem (2nd version)

If p is prime, then for all integers a,

$a^p \equiv a \bmod p$

Fermat little theorem (1st version)

If p is prime, then for all integers a coprime to p, $a^{p-1} \equiv 1 \bmod p$

3.14. We stated that the number 561 is a Carmichael number, but we never checked that $a^{561} \equiv a \pmod{561}$ for every value of a.

(a) The number 561 factors as $3 \cdot 11 \cdot 17$. First use Fermat's little theorem to prove that

$$a^{561} \equiv a \pmod 3, \quad a^{561} \equiv a \pmod{11}, \quad \text{and} \quad a^{561} \equiv a \pmod{17}$$

for every value of a. Then explain why these three congruences imply that $a^{561} \equiv a \pmod{561}$ for every value of a.

(a) By Fermat's little theorem

$a^2 \equiv 1 \bmod 3$

$a^{10} \equiv 1 \bmod 11$

$a^{16} \equiv 1 \bmod 17$

$a^{561} \equiv a^{561 \bmod 2} \equiv a \bmod 3 \rightarrow 3 \mid a^{561} - a$

$a^{561} \equiv a^{561 \bmod 10} \equiv a \bmod 11 \rightarrow 11 \mid a^{561} - a$

$a^{561} \equiv a^{561 \bmod 16} \equiv a \bmod 17 \rightarrow 17 \mid a^{561} - a$

Using the fact that if $a \mid c$ and $b \mid c$ and $\gcd(a,b) = 1$, then $ab \mid c$.

We have $3.11.17 \mid a^{561} - a$

so, $a^{561} \equiv a \bmod 3.11.17$