Exrercise 6.1

(i) $x^2 \equiv 1 \pmod p \Leftrightarrow 1 = x^2 + pk$ for $k \in \mathbb{Z}$.

$\Leftrightarrow (x+1)(x-1) \equiv 0 \pmod p$

$\Leftrightarrow p \mid x+1 \ \vee \ p \mid x-1$

$\Leftrightarrow x \equiv \pm 1 \pmod p$

(ii) Each a in $\{1 \cdots p-1\}$ has an inverse $a^* \in \{1 \cdots p-1\}$ modulo p. modulo p, that satisfies $aa^* \equiv 1 \pmod p$. This inverse is unique and follows that $(a^*)^* = a$. If $a = a^*$, then $a^2 \equiv 1 \pmod p$.

From i) we know that $a \equiv \pm 1 \pmod p$

a can only be 1 or $p-1$.

In the product $(p-1)! = 1 \times \cdots (p-1)$, we pair of each term save for 1 and $p-1$ with its inverse modulo p.

$(p-1)! \equiv 1 \times (p-1) \equiv -1 \pmod p$

(iii) As $(p-1)! \equiv -1 \pmod p$

Since $p \equiv 3 \pmod 4$, every integer from $1 \cdots \frac{p-1}{2}$ can be reached.

$1 \equiv -(p-1)$, $2 \equiv -(p-2) \cdots \frac{p-1}{2} \equiv -\frac{p+1}{2}$

So $\left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{p-1}{2}} \frac{(p-1)!}{\left(\frac{p-1}{2}\right)!} \pmod p$, then $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv 1 \pmod p$

iv) Let p be a prime and $n=p-1$

$n!+1 \equiv 0 \pmod p$, and $(p-1)!+1 > p$ for $p \geq 5$

And these $n!+1$ are composite.

Excercise 6.2

$p(x) = a_0 + a_1 x + \cdots a_n x^n \quad a_0 \cdots a_n \in \mathbb{Z}/p\mathbb{Z}$

For prime p:

We choose the smallest n so that $p(x)$ has more than n roots.

roots: $r_1 \cdots r_{n+1}$.

$p(x) - p(r_1) = (x-r_1) q_x \quad q_x$ is at most $n-1$ degree.

Since $p(x)$ has more than n roots, $q(x)$ has at least n roots.

And this lead to the contradiction

Ve203 Discrete Mathematics (Fall 2022)

Assignment 6

Date Due: See canvas
This assignment has a total of **(35 points)**.
Note: Unless specified otherwise, you must show the details of your work via logical reasoning for each exercise. Simply writing a final result (whether correct or not) will receive **0 point**. **Explain** (briefly) if you claim something is trivial or straightforward. Provide a counterexample if you are trying to disprove something. It is **NOT OK** to write something like "how do we know that blahblahblah is even true..." In addition, be careful that some problems might be ill-defined.

Exercise 6.1 (7 pts) Given $p \in \mathbb{P}$, show that

(i) (1 pt) $x^2 \equiv 1 \pmod{p}$ iff $x \equiv \pm 1 \pmod{p}$.

(ii) (2 pts) (Wilson's theorem) $(p-1)! \equiv -1 \pmod{p}$.

(iii) (2 pts) If $p \equiv 3 \pmod{4}$, then $\left(\dfrac{p-1}{2}\right)! \equiv \pm 1 \pmod{p}$.

(iv) (2 pts) Use (ii) to show that there are infinitely many composite numbers of the form $n! + 1$.

Exercise 6.2 (2 pts) Given $p \in \mathbb{P}$, consider the polynomial p of degree n given by

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n, \qquad a_0, \ldots, a_n \in \mathbb{Z}/p\mathbb{Z}$$

show that p has at most n roots in $\mathbb{Z}/p\mathbb{Z}$. (Hint: factor p and use induction.)

Exercise 6.3 (2 pts) Apply Chinese remainder theorem to show that $a^{561} \equiv a \pmod{561}$ for all $a \in \mathbb{Z}$.

Exercise 6.4 (6 pts) Given $p, q \in \mathbb{P}$, $a \in \mathbb{Z}$, show that

(i) (2 pts) If $a^q \equiv 1 \pmod{p}$, then either $p \equiv 1 \pmod{q}$ or $a \equiv 1 \pmod{p}$.

(ii) (2 pts) If $5 \mid a$ and $p \mid a^4 + a^3 + a^2 + a + 1$, then $p \equiv 1 \pmod{5}$.

(iii) (2 pts) Use (ii) to show that there are infinitely many primes of the form $10n + 1$, $n \in \mathbb{N}$.

Exercise 6.5 (2 pts) Find prime factors of $F_5 = 2^{2^5} + 1$ by applying Fermat's theorem.

Exercise 6.6 (2 pts) Show that 2077 is not prime by Fermat test.

Exercise 6.7 (2 pts) Sove the following system of linear congruence

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{4} \\ x &\equiv 4 \pmod{5} \\ x &\equiv 5 \pmod{6} \\ x &\equiv 6 \pmod{7} \end{aligned}$$

Exercise 6.8 (4 pts)

(i) (2 pts) Show that $6x \equiv 2 \pmod{3}$ has no solutions.

(ii) (2 pts) Show that $6x \equiv 2 \pmod{5}$ has infinitely many solutions.

Exercise 6.9 (6 pts) Given public key $(n, E) = (2077, 97)$, where $2077 = 31 \times 67$.

(i) (2 pts) Encrypt the message 1984 by the encryption function $e(x) = x^E \pmod{n}$.

(ii) (2 pts) Compute the private key $D = E^{-1} \pmod{\varphi(n)}$.

(iii) (2 pts) Decrypt the encrypted message in (i) using Chinese remainder theorem. Is it possible to do the encryption in (i) using Chinese remainder theorem?

Exercise 6.10 (2 pts) Is the group $(\mathbb{Z}/12\mathbb{Z})^{\times}$ is cyclic? Explain.

Excercise 6.9

(i) $e(x) = x^E \pmod n$

$E = 97,\ n = 2077$

$e_{1984} = 1984^{97} \pmod{2077}$

$$
\begin{aligned}
1984^{97} \pmod{2077} &= 341^{48} \cdot 1984 \pmod{2077} \\
&= 961^{12} \cdot 1984 \pmod{2077} \\
&= 1581^{4} \cdot 1984 \pmod{2077} \\
&= 930^{2} \cdot 1984 \pmod{2077} \\
&= 868 \times 1984 \pmod{2077} \\
&= 279 \pmod{2077}
\end{aligned}
$$

(ii)

$DE = 1 \bmod (\varphi(n))$

$\varphi(2077) = \varphi(31)\varphi(67) = 30 \times 66 = 1980$

$97D \equiv 1 \pmod{1980}$

$97D + 1980k = 1$

$D = -347 \equiv 1633 \pmod{1980}$

Ecludien

$1980 = 97 \times 20 + 40$

$97 = 40 \times 2 + 17$

$40 = 17 \times 2 + 6$

$17 = 2 \times 6 + 5$

$6 = 5 \times 1 + 1$

Back tracing

$$
\begin{aligned}
1 = 6 - 5 &= 6 - (17 - 2\times 6) = 6 \times 3 - 17 \\
&= (40 - 17 \times 2) \times 3 - 17 \\
&= 40 \times 3 - 17 \times 7 \\
&= 40 \times 3 - (97 - 40 \times 2) \times 7
\end{aligned}
$$

$40 \times 17 - 97 \times 7$

$= 1980 \times 27 - 97 \times 347$

Excercise 6.3

if

gcd (a, 3) = 1,

$a^{561} \equiv (a^2)^{280} \cdot a \equiv a \pmod{3}$

similarly

$a^{561} \equiv (a^{10})^{56}\, a \equiv a \pmod{11}$

if $11 \mid a$ $\quad a^{561} \equiv 0 \equiv a \bmod (11)$

$a^{561} \equiv (a^{16})^{35}\, a \equiv a \bmod (17)$

$$\begin{cases} a^{561} \equiv a \pmod{3} \\ a^{561} \equiv a \pmod{11} \\ a^{561} \equiv a \pmod{17} \end{cases}$$

$a^{561} \equiv a \pmod{3 \times 11 \times 17} \equiv a \pmod{567}$

Excercise 6.4

i) $a^{p-1} \equiv 1 \pmod{p}$, if gcd$(a,p) = 1$ (which is true)

$a^q \equiv 1 \pmod{p}$ $\qquad$ if $p \equiv 1 \pmod{q}$, then proved

$a^{p(q-1)} \equiv 1 \pmod{p}$. $\qquad$ if $p \not\equiv 1 \pmod{q}$, $a' \equiv 1 \pmod{p}$

ii) $\frac{a^5-1}{a-1} \equiv 0 \pmod p$

$a^5 \equiv 1 \pmod p$

As $a^{p-1} \equiv 1 \pmod p$

So $a^{(p-1,5)} \equiv 1 \pmod p$

If $a \equiv 1 \pmod p$, $a^4+\cdots 1 = 5 \pmod p$

So $p=5$. However $5|a \Rightarrow 5 \nmid a^5-1$ contradicts

So $a \not\equiv 1 \pmod p$. So $p \equiv 1 \pmod 5$

iii) Choose $a_1 = 5$, $a_n = a_1 \cdots a_{n-1} + 1$

So with different a, $a^4 + \cdots a + 1$ is different.

but each has a distinct factor p.

This is because $a_n^4 + \cdots a_n + 1 \equiv 5 \pmod{a_2}$

and $p \neq 5$

So $a_i \nmid a_n^4 + \cdots 1$.

So $a_n^4 + \cdots 1$ has distinct prime factor

p, $p \equiv 1 \pmod{10}$