Tutorial Group 4

Exercise 3.4.4

If $p = 4n+1$ is prime, then $[(2n)!]^2 \equiv -1 \pmod{p}$.

Proof: (direct)

Fix n in $\mathbb{N}$ such that $4n+1$ is prime and call that prime p.

First observe by Wilson's Theorem $(4n)! \equiv -1 \pmod{p}$.

Also note $(4n)! = (4n)(4n-1)\ldots(2n+1)(2n!)$.

Now $p \equiv 0 \pmod{p}$, so $p+j \equiv j \pmod{p}$ for any integer j.

From this, $4n+1+j \equiv j \pmod{p}$ and so $2n+j \equiv -2n+j-1 \pmod{p}$.

So $\prod_{1 \le i \le 2n} 2n+i \equiv \prod_{1 \le i \le 2n} -2n+i-1 \pmod{p}$.

Note $\prod_{1 \le i \le 2n} 2n+i = (2n+1)(2n+2)\ldots(4n) = \frac{(4n)!}{(2n)!}$.

Also $\prod_{1 \le i \le 2n} -2n+i-1 = (-1)^{2n} \prod_{1 \le i \le 2n} 2n+1-i = (2n)(2n-1)\ldots(1) = (2n)!$.

So $(2n)! \equiv \frac{(4n)!}{(2n)!} \pmod{p}$ or $[(2n)!]^2 \equiv (4n)! \equiv -1 \pmod{p}$.

QED

Group 2

10/28

3.4.5

Proof: (Direct)

Fix p an odd prime and n, a positive integer less than p.

We know $(p-1)! = (p-1)(p-2)\cdots(p-(n-1))(p-n)!$ And

$(p-1)(p-2)(p-3)\cdots(p-(n-1)) \equiv (-1)(-2)(-3)\cdots(-(n-1)) \pmod{p}$

in the order given. We can write

$(-1)(-2)(-3)\cdots(-(n-1)) = (n-1)!(-1)^{n-1}$. So

$(p-1)! \equiv (p-n)!(n-1)!(-1)^{n-1} \pmod{p}$. We also

know $(p-1)! \equiv (-1) \pmod{p}$ by Wilson's Thm.

So $(p-n)!(n-1)!(-1)^{n-1} \equiv -1 \pmod{p}$. We know

$[(-1)^{n-1}][(-1)^{n-1}] = -1^{2n-2} = 1$. So

$(p-n)!(n-1)! \equiv (-1)^n \pmod{p}$. ∎

Group 1

3.5.3.

To prove: If p is prime, then

$$1^{(p-1)} + 2^{(p-1)} + \dots + (p-1)^{(p-1)} + 1 \equiv 0 \pmod{p}$$

Proof (Direct): Fix p a prime in $\mathbb{N}$. Let $a_1 = 1, a_2 = 2, \dots, a_{p-1} = p-1$

Using Fermat's little theorem we know that

$1^{p-1} \equiv 1 \pmod{p}$, $2^{(p-1)} \equiv 1 \pmod{p} \dots, (p-1)^{(p-1)} \equiv 1 \pmod{p}$

Since $(a_i, p) = 1$.

Then we also have:

$$(p-1)\cdot(1) + 1 \equiv p(1) \equiv 0 \pmod{p}$$

So, $1^{(p-1)} + 2^{(p-1)} + \dots (p-1)^{(p-1)} + 1 \equiv 1 \pmod{p}$

Proved

Group 3

Exer. 3.6.6

Proof (Direct):
Fix n in $\mathbb{N}$ with $n = p_1^{k_1} \cdots p_r^{k_r}$.
Let $\phi(n) = p_1^{k_1-1}(p_1-1) \cdots p_r^{k_r-1}(p_r-1)$.

Case 1: Fix $p_1, \ldots, p_r$ all odd primes.
Each prime can be written as $2x_i+1$ with $x > 0$.

$$\phi(n) = p_1^{k_1-1}((2x_1+1)-1) \cdots p_r^{k_r-1}((2x_r+1)-1)$$

$$\phi(n) = 2^r[p_1^{k_1-1}(x_1) \cdots p_r^{k_r-1}(x_r)].$$

So $2^r \mid \phi(n)$, therefore $2^{r-1} \mid \phi(n)$.

Case 2: Fix $p_1 = 2$ and $p_2, \ldots, p_r$ as odd primes expressed as $2x_i+1$.

$$\phi(n) = 2^{k_1-1}(2-1)p_2^{k_2-1}((2x_2+1)-1) \cdots p_r^{k_r-1}((2x_r+1)-$$

$$\phi(n) = 2^{r-1}[2^{k_1-1}p_2^{k_2-1}(x_2) \cdots p_r^{k_r-1}(x_r)]$$

So $2^{r-1} \mid \phi(n)$. ∎