Midterm Practice

Problem 1

- Find a prime factor of $(5^{15}-1)/4$

$$
\begin{aligned}
5^{15}-1 &= \frac{5-1}{4}(5^{14}+5^{13}+\cdots) \\
(5^3)^5-1 &= \frac{5^3-1}{4}(5^{12}+5^9+\cdots) \\
\frac{5^3-1}{4} &= \frac{5-1}{4}(5^2+5+1) = 31
\end{aligned}
$$

- $x^n-1=(x-1)(x^{n-1}+x^{n-2}+\cdots)$ is a useful equation
- You want to make sure you're working with the smallest exponent possible to reduce the amount of time you're spending on the problem
  - i.e. reducing 5^3 instead of 5^5 which would've given the same answer but taken more time
- Remember polynomial factorization

Problem 2

- If a group in G, an element g has order 169. What is the order of g^{51}?

$$g^a = \frac{ord(g)}{gcd(a, ord(g))}$$

$$
\begin{aligned}
ord(g^{51}) &= \frac{ord(g)}{gcd(51, ord(g))} \\
&= \frac{169}{gcd(51,169)} \\
&= 169
\end{aligned}
$$

Problem 3

- Calculate the subgroup generated by x in $(\mathbb{F}_2[x]/(x^3+x+1))*$

$$
\begin{aligned}
&x \\
&x^2 \\
&x^3 = x+1 \\
&x^4 = x^2+x \\
&x^5 = x^3+x^2 = x^2+x+1 \\
&x^6 = x^3+x^2+x = x^2+1 \\
&x^7 = x^3+x = 1
\end{aligned}
$$

* What we did in class confused me, so here's how I explained it to myself. It's probably a little wrong but I think it'll work

x generated by $(\mathbb{F}_2[x]/x^3+x+1)^*$

x
x^2
$x^3 = x+1$
$x^4 = x^2 + x$
$x^5 = x^3 + x^2 = x^2 + x + 1$
$x^6 = x^3 + x^2 + x = x^2 + 1$
$x^7 = x^3 + x = 1$

Polynomial: x^3+x+1
Start w/: $x^3 = x+1$
End w/: $1 = x^3 + x$

Factoring:

$x^5 = x^3 + x^2$
$= x^2(x^3/x^2 + 1)$
$= x^2(x^{3-2} + 1)$
$= x^2(x+1)$
$= x^2 + x + 1$ // in $\mathbb{F}_2[x]$

$x^6 = x^3 + x^2 + x$
$x(x^2 + x + 1)$
$= x^2 + 1$ // in $\mathbb{F}_2[x]$

Problem 4

- Compute the multiplicative inverse of $x^6 + 1$ modulo $x^8 + x^4 + x^3 + x + 1$ over $\mathbb{Z}/2\mathbb{Z}$ using Extended Euclidean Algorithm. You need to show steps
- Extended Euclidean Algorithm:

  $$Au + bvgcd(A, B)$$

  can be changed to

  $$\frac{A}{gcd(A,B)}u + \frac{B}{gcd(A,B)}v = 1$$

- You basically continue to take the divide $x^6 + 1$ by $x^8 + x^4 + x^3 + x + 1$ until you come up with the polynomial such that $x^8 + x^4 + x^3 + x + 1 \div x^6 + 1 = 1$, I think anyways…I really don't know
- Godspeed for this problem

Problem 5

- Compute $18^{20^{20}} \bmod 28$
- Use the chinese remainder theorem

$$
\begin{aligned}
28 &= 4 \times 7 \\
18^{20^{20}} \bmod 4 &= 2 \\
2^{20^{20}} &= 0 \\
18^{20^{20}} \bmod 7 &= 4 \\
&= 4^{2^{2} \bmod 6} \\
&= 4^4 \bmod 7 \\
&= 4
\end{aligned}
$$

- mod4 didn't work because 18 mod 4 = 2 and $2^{20^{20}} = 0$ in this...ring? So this means 4 is a zero divisor and we should try mod7
- 18 mod 7 = 4 so we're good there
- You can ignore the exponents and focus on the base when taking the mod
- $4^{2^{20} \bmod 6} = 4$ because 4 mod 6 = 4
- $4^4 \bmod 7 = 4$ because 4 mod 7 = 4
- I don't know where the exponents came from but I don't think it really matters since you're ignoring them the whole time
- Aside: How to calculate x mod y
  - Divide x by y (in our case, $18 \div 7$)
  - Round this number down (in our case, $18 \div 7 \approx 2$)
  - Multiply this number by y (in our case, $7 \times 2 = 14$)
  - Subtract the product from x (in our case, $18 - 14 = 4$)
  - That's the remainder!

Problem 6

- Compute $\phi(50)$

$$
\begin{aligned}
\phi(p) &= p - 1 \text{ where p is a prime number} \\
\phi(p^m) &= p^m - p^{m-1} \text{ where p is a prime number} \\
\phi(p, q) &= (p-1)(q-1) \\
\phi(m, n) &= \phi(m) \times \phi(n)
\end{aligned}
$$

$$
\begin{aligned}
&\text{50 is not prime, so:} \\
&50 = 5 \times 5 \times 2 \\
\phi(50) &= \phi(5 \times 5 \times 2) \\
&= \phi(5^2 \times 2) \\
&= \phi(5^2) \times \phi(2) \\
&= \phi(5^2) - 1 \\
&= (5^2 - 5^1) \times 1 \\
&= (25 - 5) \times 1 \\
&= 20
\end{aligned}
$$