MATH 314 Spring 2020 - Class Notes

2/19/2020

Scribe: Shania Foster

Summary: Today in class we covered Euler Phi Function and Euler's Theorem.

Notes:

Fermat's Little Theorem:
Does not work if modulus is not prime.

Take n = 6, a = 4
$a^{n-1} \equiv 4^5 \equiv 4^4 * 4$
Hint: $4^4 \equiv 4 \pmod 6$

Euler's Phi Function (or Euler's Totient Function):

φ(n) = number of reminders $\pmod{n}$ have an inverse
= number [a $\pmod{n}$ or gcd(a,n) = 1]

Examples:
$\varphi(26) = 12$

$\varphi(10) = 4$
0,1,2,3,4,5,6,7,8,9 *Cross out numbers without inverses*
This leaves 1,3,7,9 left
Hint: If gcd is not 1, then no inverse. So (5,10) = 5 so 5 gets crossed out

$\varphi(7) = 6$
0,1,2,3,4,5,6 *Cross out 0*
This leaves 1,2,3,4,5,6 left

φ(p) = p-1
$\varphi(9) = \varphi(3^2) = 6$
Above, you have 0,1,2,3,4,5,6,7,8. You would need to cross out 0,3,and 6. That leaves 1,2,4,5,7,8.

$\varphi(27) = \varphi(3^3) = 18$
Above, you have 0-26. You would need to cross out 0,3,6,9,12,15,18,21,24 That leaves 1,2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26.

$\varphi(81) = \varphi(3^4) = 18*3 = 54$

$\varphi(3^n)3^{n-1} = 3^{n-1}(3-1)$

$\varphi(p^a) = p^{a-1}(p-1)$

$\varphi(\text{p q}) = \varphi(p)\varphi(q)$

$\varphi(\text{n m}) = \varphi(n)\varphi(m)$ *if gcd(m,n) = 1*

$\varphi(10) = \varphi(2*5) = \varphi(2)\varphi(5) = 1*4 = 4$

$\varphi(26) = \varphi(2)\varphi(13) = 1*12 = 12$

$\varphi(60) = \varphi(5 * 12) = \varphi(5)\varphi(12)$
$= \varphi(5)\ \varphi(4)\ \varphi(3)$
Side Note: $\varphi(4) = \varphi(2^2) = 2^1\ (2-1) = 2$
$= (4)*(2)*(2)$
$= 16$

$\varphi(100) = \varphi(2^2 * 5^2) = \varphi(2^2) * \varphi(5^2)$
$= 2(20) = 40$

Definitions

- m and n are <u>coprime</u> if gcd(m,n) = 1
- a $\pmod n$ is a <u>residue</u> $\pmod n$

Euclear Theorem: (Fermat's Little Theorem of Composite n)

If gcd (a,n) = 1 then $a^{\varphi(n)} \equiv 1 \pmod n$

If n = p is prime $\varphi(p)$ = p-1 we get Fermat's Theorem.

<u>**Example:**</u>
n = 10, a = 3
gcd(3,10) = 1
Eucler: $3^{\varphi(10)} \pmod{10}$
$\equiv 3^4 \equiv 81 \equiv 1 \pmod{10}$

Updated General Principle of modular exponents If we're working $\pmod{n}$
work $\pmod{\varphi(n)}$ in the exponent.

If we have a ring (add, subtract, multiply) where we are also allowed to divide by everything but 0, this is called a Field.

Example:
Integers don't work (5/2 not an integer) and neither do polynomials 1/x
Rational Numbers
Complex Numbers
Real Numbers
Integers $\pmod{p}$ $\mathbb{F}$p *(Side Note: The P is prime)*

$\mathbb{F}$p is called a Finite Field (or Galois Field)

Are there any fields with finitely many things in them that aren't integers $\pmod{p}$?
Is there a field with 4 elements?

Integers $\pmod{4}$ are not a field.

Addition $\pmod{4}$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Multiplication $\pmod{4}$

x	0	1	2	3	
0	0	0	0	0	
1	0	1	2	3	
2	**0**	**2**	**0**	**2**	*Not a field*
3	0	3	2	1	

Polynomials with coefficients $\pmod{2}$ $\mathbb{F}$2[x]

$g(x) = 1 * x^3 + 1 * x^2 + 0 * x + 1$
$= x^3 + x^2 + 1$

$f(x) = x^4 + x^2$

f(x)+g(x) $= (x^3 + x^2 + 1) + (x^4 + x^2)$ *(x^2 cancels out)*

$=x^4+x^3+1$

f(x)g(x) $=(x^3+x^2+1)(x^4+x^2)$
$=(x^7+x^6+x^4)+(x^5+x^4+x^2)$ *(x^4 cancels out)*
$=x^7+x^6+x^5+x^2$

(mod 2) Addition and Subtraction are the same

f(x)-g(x) $=(x^4+x^2)-(x^3+x^2+1)$
$=x^4-x^2-1=x^4+x^3+1$

$\mathbb{F}2[x]$ is a ring

f(x) = x has no inverse
You can still do division of polynomials with remainder

$$
\begin{array}{r|rrrrr}
 & & & & x & -1 \\ \cline{2-6}
x^3+x^2+1 & x^4 & & +x^2 & & \\
 & -x^4 & -x^3 & & -x & \\ \cline{2-5}
 & & -x^3 & +x^2 & -x & \\
 & & x^3 & +x^2 & & +1 \\ \cline{3-6}
 & & & 2x^2 & -x & +1
\end{array}
$$

So $x^4+x^2 \equiv (x+1) \pmod{x^3+x^2+1}$

<u>**Example:**</u> Find what x^5+x+1 is $\pmod{x^3+x^2+1}$

$$
\begin{array}{r|rrrrrr}
 & & & & x^2 & -x & +1 \\ \cline{2-7}
x^3+x^2+1 & x^5 & & & & +x & +1 \\
 & -x^5 & -x^4 & & -x^2 & & \\ \cline{2-5}
 & & -x^4 & & -x^2 & +x & \\
 & & x^4 & +x^3 & & +x & \\ \cline{3-6}
 & & & x^3 & -x^2 & +2x & +1 \\
 & & & -x^3 & -x^2 & & -1 \\ \cline{4-7}
 & & & & -2x^2 & +2x &
\end{array}
$$

So $x^{5+x+1} \equiv 0 \pmod{x^3+x^2+1}$