tags: ***MATA02-2022***

MATA02-2022: Quiz 5 practice [20pts total]

During tutorials week 12: April 4-8

1. Roots [12pts]

- For each of the following three root problems, one of them will be solveable using the method with Fermat's Little Theorem, one of the remaining two will be solveable using the method with Euler's Theorem, and the one left over will not be solveable using either method.
- Solve the two problems that are solveable using those two methods.
- Say why the left over problem cannot be solved using either of the two methods.

1. $\sqrt[12]{7}$ mod 61
2. $\sqrt[5]{3}$ mod 23
3. $\sqrt[13]{8}$ mod 57

1. $\sqrt[12]{7} \mod 61$

61 is prime, and $\gcd(7,61)=1$, but $\gcd(12,60)=12$,

we cannot use either method.

2. $\sqrt[5]{3} \mod 23$

23 is prime, and $\gcd(3,23)=1$, and $\gcd(5,22)=1$,

so we can use Fermat's Little Thm to find the root.

$22 = 5\cdot 4+2$

$5 = 2\cdot 2+1$

$1 = 5-2\cdot 2$

$1 = 5-(22-5\cdot 4)\cdot 2$

$1 = 5\cdot 9 - 22\cdot 2$

Thus, $3^1 \equiv 3^{45}$

$\Rightarrow \sqrt[5]{3^1} \equiv \sqrt[5]{3^{45}} \equiv 3^9$

$\equiv 3^1\cdot 3^8 \equiv 3\cdot 6 \equiv \boxed{18 \mod 23}$

$3^1 \equiv 3$

$3^2 \equiv 9$

$3^4 \equiv 81 \equiv 12$

$3^8 \equiv 144 \equiv 6$

Extra space for problem 1

3. $\sqrt[13]{8} \mod 57$

57 is not prime, so we cannot use Fermat

$57 = 3 \cdot 19$

$\phi(57) = 57 \cdot \frac{2}{3} \cdot \frac{18}{19} = 36$

$\gcd(8, 57) = 1$ and $\gcd(13, 36) = 1$, so can use Euler to find roots

$36 = 13 \cdot 2 + 10$
$13 = 10 \cdot 1 + 3$
$10 = 3 \cdot 3 + 1$

$1 = 10 - 3 \cdot 3$

$1 = 10 - (13 - 10) \cdot 3$

$1 = 10 \cdot 4 - 13 \cdot 3$

$1 = (36 - 13 \cdot 2) \cdot 4 - 13 \cdot 3$

$1 = 36 \cdot 4 - 13 \cdot 11$

$$8^1 \equiv 8^{1 - 36 \cdot 4} \equiv 8^{-13 \cdot 11}$$

$$\sqrt[13]{8} \equiv \sqrt[13]{8^{-13 \cdot 11}} \equiv 8^{-11} \equiv 8^{-11+36} \equiv 8^{25}$$

$$\equiv 8^{16} \cdot 8^{8} \cdot 8$$

$$\equiv -8 \cdot 7 \cdot 8$$

$$\equiv -64 \cdot 7$$

$$\equiv -7 \cdot 7$$

$$\equiv -49$$

$$\boxed{\equiv 8 \mod 57}$$

$8^1 \equiv 8 \mod 57$
$8^2 \equiv 64 \equiv 7$
$8^4 \equiv 49 \equiv -8$
$8^8 \equiv 64 \equiv 7$
$8^{16} \equiv 49 \equiv -8$

2. Fermat Primality Testing [8pts]

We know 41 is a prime number from the Sieve of Eratosthenes. But if you didn't know that, one way to show that it is probably prime is to use the Fermat Primality Test.

Using Fermat's primality test, show that with probability at least $1/8$, 41 is prime.

Need to check $a^{40} \equiv 1 \mod 41$

for 3 different random a's.

$$a^{40} \equiv a^{32+8}$$

Let $a = 2$

$2^1 \equiv 2$

$2^2 \equiv 4$

$2^4 \equiv 16$

$2^8 \equiv 256 \equiv 10$

$2^{16} \equiv 100 \equiv 18$

$2^{32} \equiv 324 \equiv -4$

$2^{40} \equiv -4 \cdot 10 \equiv -40 \mod 41$

$\equiv 1 \mod 41.$

Let $a = 3$

$3^1 \equiv 3$

$3^2 \equiv 9$

$3^4 \equiv 81 \equiv -1$

$3^8 \equiv 1$

$3^{16} \equiv 1$

$3^{32} \equiv 1$

$3^{40} \equiv 1 \cdot 1 \equiv 1 \mod 41$

Let $a = 4$

$4^1 \equiv 4$

$4^2 \equiv 16$

$4^4 \equiv 256 \equiv 10$

$4^8 \equiv 100 \equiv 18$

$4^{16} \equiv 324 \equiv -4$

$4^{32} \equiv 16$

$4^{40} \equiv 16 \cdot 18$

$\equiv 288 \equiv 1 \mod 41$

Thus, 41 passes Fermat's primality test 3 times.

Extra space for problem 2