2017

Problem 1 (16 points)

(a, 4pts) True or false: $\forall a \in \mathbb{Z}_{11}, a \neq 0$: $(a^5 \bmod 11) \in \{1, 10\}$. Please explain.

TRUE

$(a^5)^2 \equiv a^{10} \equiv 1 \pmod{11}$

$\Rightarrow a^5 \equiv \pm 1 \equiv 1$ or $10 \pmod{11}$

(b, 4pts) True or false: $41041 = 7 \cdot 11 \cdot 13 \cdot 41$ is a Carmichael number. Please explain.

TRUE

$7-1=6 \mid 41041-1 = 41040$ bec. $3 \mid 41040$

$11-1=10 \mid 41040$, $13-1=12 \mid 41040$ bec $4 \mid 41040$

$41-1=40 \mid 41040$ bec $8 \mid 41040$

(c, 4pts) Please compute $2^{50} \bmod 25$, showing your work.

$GCD(2,25)=1 \Rightarrow 2^{\phi(25)} = 2^{20} \equiv 1 \pmod{25}$

$2^{50} = 2^{40+10} = (2^{20})^2 \cdot 2^{10} \equiv 2^{10} \pmod{25}$

$2^{10} = 1024 \equiv 24 \pmod{25} \Rightarrow 2^{50} \equiv 24 \pmod{25}$

(d, 4pts) Please compute the values of the number theoretic functions $\tau(70)$, $\mu(70)$ and $\sigma(70)$.

$70 = 2^1 \cdot 5^1 \cdot 7^1$

$\tau(70) = (1+1)(1+1)(1+1) = 8$

$\mu(70) = (-1)^3 = -1$

$\sigma(70) = 1+2+5+7+10+14+35+70 =$
$(1+2)(1+5)(1+7) = 144$

2017

Problem 2 (6 points): A Mersenne number is an integer of the form $2^p - 1$, where p is a prime number. Note that the Mersenne number $2^{11} - 1 = 23 \cdot 89$ is not a prime number. Please prove that the only Mersenne number that is divisible by 7 is $2^3 - 1$.

$2^2 - 1 = 3$

$2^3 - 1 = 7$

$2^3 \equiv 1 \pmod 7$ $\quad 2^{3+6k} \equiv 1 \pmod 7$

$2^5 \equiv 4 \pmod 7$ $\quad 2^{5+6k} \equiv 4 \pmod 7$

$2^7 \equiv 2 \pmod 7$ $\quad 2^{1+6k} \equiv 2 \pmod 7$

$2^9 \equiv 1 \pmod 7$

If $p = 1+6k$ then $2^p - 1 \equiv 1 \pmod 7$

$p = 5+6k$ then $2^p - 1 \equiv 3 \pmod 7$

No other primes $p \geq 5$

Problem 3 (6 points): Please determine an integer $n \geq 1$ such that $\phi(n) < \frac{n}{3}$, where ϕ is Euler's phi-function. Please show your work.

$$\phi(n) = n \cdot \underbrace{\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right)}_{< \frac{1}{3}}$$

$$\underbrace{\left(1 - \frac{1}{2}\right)}_{\frac{1}{2}} \underbrace{\left(1 - \frac{1}{3}\right)}_{\frac{2}{3}} \underbrace{\left(1 - \frac{1}{5}\right)}_{\frac{4}{5}} = \frac{1}{3} \cdot \frac{4}{5} < \frac{1}{3}$$

$n = 2 \cdot 3 \cdot 5 = 30$ $\quad \phi(30) = 8 < \frac{30}{3} = 10$

$n = 2 \cdot 3 \cdot 7 = 42$ $\quad \phi(42) = 2 \cdot 3 \cdot 7 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{6}{7} = 12 < 14$

Problem 4 (8 points): Consider $1260 = 4\cdot 5\cdot 7\cdot 9$ and let $a \in \mathbb{Z}_{1260}$ with

$$\begin{aligned} a &\equiv 3 \pmod{4},\\ a &\equiv 1 \pmod{5},\\ a &\equiv 5 \pmod{7},\\ a &\equiv 4 \pmod{9}. \end{aligned}$$

Please compute $y_0 \in \mathbb{Z}_4$, $y_1 \in \mathbb{Z}_5$, $y_2 \in \mathbb{Z}_7$ and $y_3 \in \mathbb{Z}_9$ such that

$$a = y_0 + y_1\cdot 4 + y_2\cdot 4\cdot 5 + y_3\cdot 4\cdot 5\cdot 7.$$

Then compute a. Please show all your work.

$y_0 = a \bmod 4 = 3$

$3 + 4\cdot y_1 \equiv 1 \pmod 5$

$y_1 \equiv (1-3)\cdot 4 \equiv 2 \pmod 5$

$3 + 4\cdot 2 + 4\cdot 5\cdot y_2 \equiv 5 \pmod 7$

$4 + 6\, y_2 \equiv 5 \pmod 7$

$y_2 \equiv (5-4)\,6 \equiv 6 \pmod 7$

$$\underbrace{3 + \underbrace{4\cdot 2}_{\equiv -1} + \underbrace{\underbrace{4\cdot 5}_{\equiv 2}\cdot 6}_{\equiv 3}}_{5} + \underbrace{\underbrace{4\cdot 5}_{2}\cdot 7}_{5}\, y_3 \equiv 4 \pmod 9$$

$$\begin{array}{cccc} 9 & & 1 & 0 \\ 5 & & 0 & 1 \\ 4 & 1 & 1 & -1 \\ 1 & 1 & -1 & 2 \end{array}$$

$(-1)9 + 2\cdot 5 = 1$

$\underbrace{2\cdot 5}_{\equiv 1}\cdot y_3 \equiv 2(4-5) \equiv -2 \equiv 7 \pmod 9$

$$a = \underbrace{3 + 2\cdot 4}_{11} + \underbrace{6\cdot 4\cdot 5}_{120} + \underbrace{7\cdot 4\cdot 5\cdot 7}_{980} = 1111$$

2017

Problem 5 (5 points): Let $k = 2^5 + 2^3 + 2^2 = 44$. Please show how one can compute $a^k \bmod n$ with 7 multiplications of residues modulo n.

1. $a^2 \bmod n = b$
2. $b^2 \bmod n = a^4 \bmod n = c$
3. $c^2 \bmod n = a^8 \bmod n = d$
4. $d^2 \bmod n = a^{16} \bmod n = e$
5. $e^2 \bmod n = a^{32} \bmod n = f$

$$((f \underset{6}{\cdot} d) \bmod n \underset{7}{\cdot} c) \bmod n = a^{44} \bmod n$$

Problem 6 (5 points): Please consider the RSA with the public modulus $n = pq$, where p is a prime with $p \equiv 2 \pmod 7$ (e.g., $p = 23$) and where q is a prime with $q \equiv 3 \pmod 7$ (e.g., $q = 17$), and with the public exponent $e = 7$. Please show that $d = \frac{3(p-1)(q-1)+1}{7}$ is an integer and that d is the private exponent for the RSA with such public moduli and public exponent 7.

The numerator $3(p-1)(q-1)+1 \equiv 3 \cdot 1 \cdot 2 + 1$
$\equiv 0 \pmod 7$

is divisible by 7.

$$e \cdot d \bmod \phi(n) = 7 \cdot \frac{3(p-1)(q-1)+1}{7} \bmod (p-1)(q-1)$$
$$= (3(p-1)(q-1)+1) \bmod (p-1)(q-1)$$
$$= 1$$ as required by the RSA.