정수론 HW3

20011759 박수민

1. $\left(\frac{101}{1987}\right)$**을 계산하시오**

$$\left(\frac{101}{1987}\right) = \left(\frac{1987}{101}\right)(-1)^{\frac{1986}{2}\cdot\frac{100}{2}}$$
$$= \left(\frac{68}{101}\right) = \left(\frac{2}{101}\right)^2\left(\frac{17}{101}\right)$$

$101 \equiv 5\ (mod\ 8)$이므로 $\frac{2}{101} = -1$,

$$\left(\frac{2}{101}\right)^2\left(\frac{17}{101}\right)$$
$$= (-1)^2\left(\frac{17}{101}\right)$$
$$= \left(\frac{101}{17}\right)(-1)^{\frac{100}{2}\cdot\frac{16}{2}}$$
$$= \left(\frac{16}{17}\right) = \left(-\frac{1}{17}\right)$$

$17 \equiv 1\ (mod\ 4)$이므로 $\left(-\frac{1}{17}\right) = 1$

$$\therefore \left(\frac{101}{1987}\right) = 1$$

2. $\boldsymbol{x^2 - 3x - 1\ \equiv 0\ (mod\ 31957)}$**은 해를 가지는가?**

$$x^2 - 3x - 1 \equiv 0\ (mod\ 31957)$$
$$4x^2 - 12x - 4 \equiv 0\ (mod\ 31957)$$
$$(2x-3)^2 - 13 \equiv 0\ (mod\ 31957)$$
$$(2x-3)^2 \equiv 13\ (mod\ 31957)$$

$2x - 3 \in \mathbb{Z}$이므로 $2x - 3 = X$라 하면

$$X^2 \equiv 13\ (mod\ 31957)$$

즉 법 31957에 대해 13의 이차잉여 여부를 구하면 된다.

$$\left(\frac{13}{31957}\right) = \left(\frac{31957}{13}\right)(-1)^{\frac{12}{2}\cdot\frac{31956}{2}} = \left(\frac{3}{13}\right) = \left(\frac{13}{3}\right)(-1)^{\frac{12}{2}\cdot\frac{2}{2}} = \left(\frac{1}{3}\right) = 1$$

즉 13은 법 31957에 대해 이차잉여 이므로 $X^2 \equiv 13\ (mod\ 31957)$에서 해가 존재하고,

$2x - 3 = X$이므로 $x = \frac{X+3}{2}$에서 적당한 X를 대입하여 정수가 되는 x를 구할 수 있다.

즉 해가 존재한다.

3. $x^2 \equiv 7\ (mod\ 787)$의 근을 구하시오

$$\left(\frac{7}{787}\right) = \left(\frac{787}{7}\right)(-1)^{\frac{786}{2}\cdot\frac{6}{2}} = -\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right)(-1)^{\frac{6}{2}\frac{2}{2}} = \left(\frac{1}{3}\right) = 1$$

이므로 일단 근이 존재한다는 것을 알 수 있다. 그리고 $787 \equiv 3\ (mod\ 4)$이므로

$787 = p = 4k+3,\ b \equiv 7^{\frac{p+1}{4}}$라 하면, $b^2 \equiv \left(7^{\frac{p+1}{4}}\right)^2 = 7^{\frac{p+1}{2}} = 7^{\frac{p-1}{2}} \cdot 7^1 \equiv b^{p-1} \cdot 7 \equiv 7\ (mod\ p)$ 이다.

즉, $b \equiv 7^{\frac{p+1}{4}}$가 근이 되며 $p = 787$이므로 $7^{\frac{787+1}{4}} = 7^{197} \equiv 105\ (mod\ 787)$이다.

나머지 근은 자연스럽게 -105가 된다.

$$\therefore \pm 105$$

4. p는 홀수인 소수일 때 1), 2)는 동치관계임을 증명하시오

1) $x^4 \equiv -1\ (mod\ p)$은 근을 가진다

2) $p \equiv 1\ (mod\ 8)$

1) => 2) : $x^4 \equiv -1\ (mod\ p)$의 임의의 한 근을 a라하면 $a^8 \equiv 1 (mod\ p)$인데 $ord_p(a) = 8$이다. 왜냐하면 귀류법을 적용하면 $a^8 \equiv 1(mod\ p)$에서 임의의 정수 $t|8$에 관해 $a^t \equiv 1(mod\ p)$가 성립해야 하는데 이는 가정에 의해 모순이기 때문이다. ($a^1 \equiv 1(mod\ p), a^2 \equiv 1(mod\ p)$은 양변에 4제곱, 제곱 했을때도 1이 나와야하나 $a^4 \equiv -1(mod\ p)$이고 $a^4 \equiv 1(mod\ p)$은 애초에 가정과 직접적으로 모순) 그리고 $a^{p-1} \equiv 1\ (mod\ p)$이므로 $8|p-1$이다. 왜냐하면 귀류법을 적용하여 $8 \nmid p-1$라 한다면 $p-1 = 8q+r$로 둘 수 있고$(1 \le r \le 8)$ $1 \equiv a^{p-1} \equiv a^{8q+r} \equiv (a^q)^8 a^r \equiv a^r\ (mod\ p)$에서 $1 \le r \le 8$이므로 $ord_p(a) = 8$와 모순이기 때문이다. 즉 $8|p-1$이므로 $p \equiv 1\ (mod\ 8)$

2) <= 1) : p가 소수이고 $8|p-1$이므로 법 p에서 위수가 8인 정수는 항상 존재한다. 왜냐하면 $F(d)$를 $ord_p(a) = d$인 모든 원소의 개수(단, $d|p-1$)이라 하면 $F(d) = p-1$이고 이는 위수가 d인 원소의 개수와 $p-1$이 동일하다는 의미이므로 일단 존재함을 나타내기 때문이다. 이때의 생성원을 a라 하면 $ord_p(a) = 8$이다. 그러므로 $a^8 \equiv 1\ (mod\ p),\ a^4 \equiv -1\ or\ 1\ (mod\ p)$에서 $ord_p(a) = 8$이므로 $a^4 \not\equiv 1\ (mod\ p),\ a^4 \equiv -1\ mod\ p$이므로 $x^4 \equiv -1\ (mod\ p)$은 근을 가진다.

5. 강하 과정을 두 번 적용하여 $557^2 + 55^2 = 26 * 12049$로 부터 소수 12049를 두 제곱수로 표현 하시오

$557^2 + 55^2 = 26 \cdot 12049$에서 $557 \equiv 11\ (mod\ 26), 55 \equiv 3\ (mod\ 26)$이다.

$557^2 + 55^2 \equiv 11^2 + 3^2 \equiv 0\ (mod\ 26)$이며 $11^2 + 3^2 = 5 \cdot 26$이다.

$(557^2 + 55^2)(11^2 + 3^2) = 26^2 \cdot 5 \cdot 12049 = (557 \cdot 11 + 55 \cdot 3)^2 + (557 \cdot 3 - 55 \cdot 11)^2$에서

$(557 \cdot 11 + 55 \cdot 3)^2 + (557 \cdot 3 - 55 \cdot 11)^2$은 26^2로 나누어 떨어지므로 이로 나누면

$$\left(\frac{557 \cdot 11 + 55 \cdot 3}{26}\right)^2 + \left(\frac{557 \cdot 3 - 55 \cdot 11}{26}\right)^2 = 5 \cdot 12049$$

$\frac{(557\cdot 11+55\cdot 3)}{26}=242, \frac{557\cdot 3-55\cdot 11}{26}=41$이므로 $242^2+41^2=5\cdot 12049$, 또 같은 방식을 반복하면

$$242\equiv 2\ (mod\ 5), 41\equiv 1(mod\ 5), 2^2+1^2=5$$
$$(242^2+41^2)(2^2+1^2)=(242\cdot 2+41\cdot 1)^2+(242\cdot 1-41\cdot 2)^2=5^2\cdot 12049$$
$$\left(\frac{242\cdot 2+41\cdot 1}{5}\right)^2+\left(\frac{242\cdot 1-41\cdot 2}{5}\right)^2=12049$$

$\frac{242\cdot 2+41\cdot 1}{5}=105, \frac{242\cdot 1-41\cdot 2}{5}=32$이므로 $105^2+32^2=12049$

$$\therefore 105^2+32^2=12049$$