MULTIPLICATIVE STRUCTURE OF $\mathbb{Z}/n\mathbb{Z}$

DONGRYUL KIM

양의 정수 n에 대해, $\mathbb{Z}/n\mathbb{Z}$는 정수들을 법 n으로 보았을 때 잉여류들의 집합이다. 예를 들어, 아주 엄밀하게 따지지 않는다면 $\mathbb{Z}/3\mathbb{Z}$는 $\{0, 1, 2\}$라 보아도 무방할 것이다. 이 집합 $\mathbb{Z}/3\mathbb{Z}$에는 덧셈과 곱셈의 구조가 있다. 위의 $\mathbb{Z}/3\mathbb{Z}$과 같은 예시에서는 $0+2=2$, $2+1=0$, $2\times 2=1$과 같은 계산을 할 수 있다. 이 글에서는 $\mathbb{Z}/n\mathbb{Z}$에서 정의된 곱셈 연산의 구조에 대해 집중적으로 탐구할 것이다.

1. Order of an element

정의 1.1. 서로소인 두 정수 n와 a에 대해 $a^{\phi(n)} \equiv 1 \pmod{n}$임은 잘 알려져 있다.(오일러의 정리) 이때 $a^k \equiv 1 \pmod{n}$인 최소의 양의 정수 k를 $k = \operatorname{ord}_n a$로 표기하고, n에 대한 a의 **위수**라 부르자.

정리 1.2. *음 아닌 정수 k에 대해, $a^k \equiv 1 \pmod{n}$일 필요충분조건은 $\operatorname{ord}_n a \mid k$인 것이다.*

Proof. 나머지 정리에 의하여

$$k = (\operatorname{ord}_n a)q + r$$

이며 $0 \le r < \operatorname{ord}_n a$인 q와 r이 존재한다. 자명히 $\operatorname{ord}_n a \mid k$와 $r = 0$은 동치이다. 또한, $a^{(\operatorname{ord}_n a)q} \equiv 1 \pmod{n}$이므로 $a^k \equiv a^r \pmod{n}$이다. 따라서 $a^r \equiv 1 \pmod{n}$과 $r = 0$이 필요충분하는 것을 증명해도 된다. 하지만 $0 \le r < \operatorname{ord}_n a$이므로 둘은 동치이다. □

따름정리 1.3. *서로소인 두 양의 정수 n과 a에 대해, $\operatorname{ord}_n a \mid \phi(n)$이다.*

연습문제 1.4. 양의 정수 k에 대해, $a^k \equiv 1 \pmod{n}$이지만, k의 임의의 약수 $d < k$에 대해 $a^d \not\equiv 1 \pmod{n}$이라고 한다. 이때 $k = \operatorname{ord}_n a$임을 보여라.

연습문제 1.5. 임의의 양의 정수 t에 대해, 다음을 증명하여라.

$$\operatorname{ord}_n(a^t) = \frac{\operatorname{ord}_n a}{\gcd(\operatorname{ord}_n a, t)}$$

연습문제 1.6. 양의 정수 n과 그와 서로소인 두 정수 a, b에 대해 $\operatorname{ord}_n a$와 $\operatorname{ord}_n b$가 서로소라면, $\operatorname{ord}_n(ab) = \operatorname{ord}_n a \operatorname{ord}_n b$임을 보여라.

연습문제 1.7. 소수 p와 정수 a에 대해 $\operatorname{ord}_p a = 3$이라 하자. 이때 $\operatorname{ord}_p(a+1) = 6$임을 보여라.

Date: July 7, 2016.

연습문제 1.8. 페르마 수 $2^{2^n}+1$의 모든 소인수는 $2^{n+1}k+1$꼴임을 증명하여라.

연습문제 1.9. 임의의 양의 정수 n에 대해 n은 $\phi(2^n-1)$을 나눔을 증명하여라.

연습문제 1.10. 소수 p와 정수 a에 대해, $a^{p-1}+a^{p-2}+\cdots+a+1$의 임의의 소인수는 p이거나 $pk+1$꼴임을 증명하여라. 이를 이용하여 $pk+1$꼴의 소수가 무한히 많음을 증명하여라.

연습문제 1.11 (IMO Shortlist 2006 N5)**.** 다음을 방정식을 만족시키는 정수 x, y가 존재하지 않음을 증명하여라.

$$\frac{x^7-1}{x-1} = y^5 - 1$$

2. Primitive roots

이 절의 목표는 단 하나이다: 임의의 소수에 대해 원시근이 존재함을 증명하는 것이다. 원시근의 존재성만으로도 우리는 이 문서의 제목인 "$\mathbb{Z}/p\mathbb{Z}$의 곱셈구조"에 대해 속 시원하게 알 수 있게 된다.

정의 2.1. 양의 정수 n과 정수 g에 대해, $\operatorname{ord}_n g = \phi(n)$이라면 g를 n**의 원시근**이라 부른다.

만약 n의 원시근이 존재한다면, $1, g, \ldots, g^{\phi(n)-1}$은 모두 다르므로

$$(\mathbb{Z}/n\mathbb{Z})^* = \{x \in \mathbb{Z}/n\mathbb{Z} : \gcd(n,x) = 1\} = \{1, g, \ldots, g^{\phi(n)-1}\}$$

임을 알 수 있다. 즉, n과 서로소인 모든 x는 $\bmod n$으로 g^k 꼴로 항상 표현 가능하게 된다. 이것이 얼마나 강력한 사실인지는 차후에 살펴보도록 하자.

그렇다면 언제 n의 원시근이 존재하는 것일까?

정리 2.2. *임의의 소수 p는 원시근을 갖는다.*

이 정리는 올림피아드에서 증명 없이 사용할 수 있는 정리이다. 따라서 이렇다는 사실만 알고 있으면 증명을 몰라도 큰 지장이 없을 것이다. 하지만 그렇다고 증명을 생략할 수는 없는 노릇이고, 중요한 아이디어도 포함되어 있으므로 아래에 증명을 길게 적어 놓았다.

보조정리 2.3. *소수 p와 정수계수 다항식 $f(x)$에 대해, $p \mid f(a)$라면 어떤 정수계수 다항식 $g(x)$가 존재하여 $f(x) \equiv (x-a)g(x) \pmod p$가 된다.*

Proof. 우선

$$f(x) - f(a) = (x-a)g(x)$$

인 정수계수 다항식 g가 존재한다. 여기서 $f(a) \equiv 0 \pmod p$이므로 $f(x) \equiv (x-a)g(x) \pmod p$이다. □

보조정리 2.4. *소수 p와 정수계수 다항식 $f(x)$에 대해, $f(x) = 0$은 $\mathbb{Z}/p\mathbb{Z}$에서 최대 $\deg f$개의 근을 갖는다.*

Proof. $f(x)$의 근들을 $x_1, \ldots, x_n$이라 하자. 그러면 보조정리 2.3에 의해 귀납적으로 어떤 $g(x)$가 존재하여

$$f(x) \equiv (x - x_1) \cdots (x - x_n) g(x) \pmod{p}$$

가 되어야 함을 알 수 있다. 그러므로 $n \leq \deg f$이다. □

정리 2.5. *소수 p와 $d \mid p-1$인 양의 정수 d에 대해, $x^d \equiv 1 \pmod{p}$는 $\mathbb{Z}/p\mathbb{Z}$에서 정확히 d개의 근을 갖는다.*

Proof. 우선

$$x^{p-1} - 1 = (x^d - 1)(x^{p-1-d} + x^{p-1-2d} + \cdots + 1) = (x^d - 1)g(x)$$

꼴로 표현 가능하다. 이때 $\deg(x^d - 1) = d$이고 $\deg(g(x)) = p - 1 - d$이므로 보조정리 2.4에 의해 각각 최대 d개, $p - 1 - d$개의 근을 갖는다. 한편 $x^{p-1} - 1$은 정확히 $p - 1$개의 근을 갖는다. 다항식 $x^{p-1} - 1$의 각각의 근들은 $x^d - 1$의 근이 되거나 $g(x)$의 근이 되어야 하는데 각각 근이 최대 $d, p - 1 - d$개이므로 $x^d - 1$은 정확히 d개의 근을 가지고 $g(x)$는 정확히 $p - 1 - d$개의 근을 가져야만 한다. □

Proof of theorem 2.2. $p - 1$을 소인수분해 하여 $p - 1 = q_1^{e_1} \cdots q_k^{e_k}$으로 표현하자. 각각의 소수 q_i에 대해, 집합

$$A_i = \{x \in \mathbb{Z}/p\mathbb{Z} : x^{(p-1)/q_i} = 1\}$$

을 정의하자. 정리 1.2에 의해 $x \in A_i$일 필요충분조건은 $\mathrm{ord}_p\, x \mid (p-1)/q_i$이고, 이것은 $q_i \mid (p-1)/(\mathrm{ord}_p\, x)$와 동치이다. 따라서 $\mathrm{ord}_p\, x = p - 1$일 필요충분조건은 $x \notin A_1, \ldots, A_k$인 것이다. 포함-배제의 원리에 의해 $\mathrm{ord}_p\, x = p - 1$인 x의 개수는

$$(p-1) - \sum_{i=1}^{k} |A_i| + \sum_{1 \leq i < j \leq k} |A_i \cap A_j| - \cdots + (-1)^k |A_1 \cap \cdots \cap A_k|$$

이다.

이제 이 값을 계산하여보자. 집합 $A_{i_1} \cap \cdots \cap A_{i_l}$은

$$\begin{aligned} A_{i_1} \cap \cdots \cap A_{i_l} &= \left\{ x \in \mathbb{Z}/p\mathbb{Z} : q_{i_1}, \ldots, q_{i_l} \mid \frac{p-1}{\mathrm{ord}_p\, x} \right\} \\ &= \left\{ x \in \mathbb{Z}/p\mathbb{Z} : q_{i_1} \cdots q_{i_l} \mid \frac{p-1}{\mathrm{ord}_p\, x} \right\} = \{x \in \mathbb{Z}/p\mathbb{Z} : x^{(p-1)/q_{i_1} \cdots q_{i_l}} = 1\} \end{aligned}$$

이므로 $|A_{i_1} \cap \cdots \cap A_{i_l}| = (p-1)/q_{i_1} \cdots q_{i_l}$이다. 따라서

$$\begin{aligned} &|(\mathbb{Z}/p\mathbb{Z}) \setminus (A_1 \cup \cdots \cup A_k)| \\ &\quad = (p-1) - \sum_{i=1}^{k} \frac{p-1}{q_i} + \sum_{1 \leq i < j \leq k} \frac{p-1}{q_i q_j} - \cdots + (-1)^k \frac{p-1}{q_1 \cdots q_k} \\ &\quad = (p-1)\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right) \cdots \left(1 - \frac{1}{q_k}\right) > 0 \end{aligned}$$

이 된다. 이것으로부터 $\mathrm{ord}_p\, x = p - 1$인 x가 존재해야 함을 알 수 있다. □

이제 연습문제를 풀며 원시근이 어떻게 사용되는지 알아보자.

연습문제 2.6. 소수 p와 임의의 정수 $0 < k < p-1$에 대해 다음을 증명하여라.

$$p \mid 1^k + 2^k + \cdots + (p-1)^k$$

연습문제 2.7. 양의 정수 n이 원시근을 갖는다면, 원시근의 개수는 $\mathbb{Z}/n\mathbb{Z}$내에서 $\phi(\phi(n))$개임을 증명하여라. 다르게 이야기하자면, 임의의 n에 대해 n의 원시근의 개수는 0 또는 $\phi(\phi(n))$임을 보여라.

연습문제 2.8. 소수 $p \equiv 2 \pmod 3$과 임의의 정수 a에 대해, $x^3 \equiv a \pmod p$는 $\mathbb{Z}/p\mathbb{Z}$에서 정확히 하나의 해를 가짐을 보여라 .

연습문제 2.9. 소수 p의 원시근 g에 대해, $g^{(p-1)/2} \equiv -1 \pmod p$임을 보여라. 이를 이용하여 $x^2 \equiv -1 \pmod p$가 $\mathbb{Z}/p\mathbb{Z}$에서 해를 가질 필요충분조건이 $p = 2$ 또는 $p \equiv 1 \pmod 4$인 것임을 보여라.

연습문제 2.10. (a) 정수 g가 소수 p의 원시근이라 하자. 이때 $g, g+p, g+2p, \ldots, g+p(p-1)$는 정확히 하나를 제외하고 모두 p^2의 원시근임을 보여라. (즉, p^2도 원시근을 갖는 것이다.)
(b) 소수 p에 대해, g가 p^2의 원시근이라면, p^3의 원시근임을 보여라. 귀납적으로 g는 임의의 $k \geq 2$에 대해 p^k의 원시근임을 보여라.
(c) 반대로, g가 p^k의 원시근이라면, 각각의 $l \leq k$에 대해 g는 p^l의 원시근도 됨을 보여라.

연습문제 2.11 (Kömal B.4401)**.** 소수 $p = 3n+1$에 대해 $1^3, 2^3, \ldots, n^3$을 p로 나눈 나머지들이 모두 다를 수 있는가?

연습문제 2.12. 합성수 m은 임의의 $\gcd(a,m) = 1$인 a에 대해 $m \mid a^{m-1} - 1$인 성질을 가지고 있다. 이때 m을 나누는 완전제곱수는 1 뿐임을 보여라. 추가로 m은 소인수를 3개 이상 가지고 있음을 증명하여라.

연습문제 2.13 (Romania TST 1996 11)**.** 임의의 정수 α에 대해 $\alpha^{3pq} \equiv \alpha \pmod{3pq}$이 성립하는 소수 p, q를 모두 구하여라.

3. Quadratic residues and the Legendre symbol

앞에 연습문제 2.9에서 우리는 -1이 $\mathbb{Z}/p\mathbb{Z}$에서 어떤 수의 제곱이 될 필요충분조건이 $p \equiv 1 \pmod 4$임을 확인했다. 여기서 더 신기한 사실은 -1을 다른 어떤 수로 바꿔도 비슷한 성질이 생긴다는 점이다. 예를 들어 5가 제곱이 될 필요충분조건은 $p \equiv \pm 1 \pmod 5$인 것이다. 더 일반적으로 p가 $4k+1$꼴의 소수일 때 p가 mod$q$로 제곱수가 되는 것과 q가 mod p로 제곱수가 되는 것이 필요충분조건이다. 이 사실은 단순히 하나의 p에 대해 $\mathbb{Z}/p\mathbb{Z}$를 관찰하는 것으로 알아낼 수 없다는 점에 그 신비로움이 더해진다. 이것을 최종 목표로 이론을 전개해나가자.

정의 3.1. 소수 $p \geq 3$에 대해 다음과 같이 **르장드르 기호**를 정의하자.

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & p \nmid a\text{이며 } x^2 \equiv a \pmod{p}\text{의 해가 존재할 경우} \\ -1 & p \nmid a\text{이며 } x^2 \equiv a \pmod{p}\text{의 해가 존재하지 않을 경우} \\ 0 & p \mid a\text{인 경우} \end{cases}$$

만약 $(a/p) = 1$이면 a를 p에 대한 **이차잉여**라 하며, $(a/p) = -1$이면 a를 p에 대한 **비이차잉여**라 한다.

정리 3.2. *소수 $p \geq 3$과 정수 a에 대해, 다음이 항상 성립한다.*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

Proof. 소수 p의 원시근 g를 아무거나 잡자. 만약 $p \nmid a$라면 $g^k \equiv a \pmod{p}$인 k가 존재한다. 여기서 k는 $\bmod p-1$로 유일하게 결정되는데, $p-1$은 짝수이므로 k의 기우성도 결정된다. k가 짝수라면, $(g^{k/2})^2 = g^k$이므로 a는 이차잉여이고, $a^{(p-1)/2} \equiv (g^{k/2})^{p-1} \equiv 1 \pmod{p}$이므로

$$\left(\frac{a}{p}\right) = 1 \equiv a^{(p-1)/2} \pmod{p}$$

가 성립한다. 반면 k가 홀수라면, 임의의 l에 대해 $(g^l)^2 = g^{2l} \not\equiv g^k \equiv a \pmod{p}$이므로 a는 비이차잉여이고, $a^{(p-1)/2} \equiv (g^{(k-1)/2})^{p-1} g^{(p-1)/2} \equiv -1 \pmod{p}$이므로

$$\left(\frac{a}{p}\right) = -1 \equiv a^{(p-1)/2} \pmod{p}$$

가 성립한다. a가 p의 배수라면, 둘 다 0이므로 성립한다. □

따름정리 3.3. *임의의 소수 $p \geq 3$와 정수 a, b에 대해 다음이 성립한다.*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Proof. 위의 정리에 의해

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$$

이 되어 성립한다. □

정리 3.4. *소수 $p \geq 3$에 대해, $p = 4k+1$꼴이라면, $(-1/p) = 1$이고, $p = 4k+3$꼴이라면, $(-1/p) = -1$이다.*

Proof. 연습문제 2.9 참조. □

정리 3.5. *소수 p에 대해, $p = 8k \pm 1$꼴이라면 $(2/p) = 1$이고 $p = 8k \pm 3$꼴이라면 $(2/p) = -1$이다.*

Proof. 정리 3.2에 의해 이것은 $2^{(p-1)/2}$를 $\bmod p$로 계산하는 문제로 귀결된다. 여기서

$$2^{(p-1)/2} = \frac{2\cdot 4\cdot\cdots\cdot(p-1)}{1\cdot 2\cdot\cdots\cdot\frac{p-1}{2}} \equiv \frac{2\cdot 4\cdot\cdots\cdot(-5)\cdot(-3)\cdot(-1)}{1\cdot 2\cdot\cdots\cdot\frac{p-1}{2}} = (-1)^{|\{k:\frac{p}{4}<k<\frac{p}{2}\}|}$$

이므로 p가 $8k\pm 1$꼴이면 우변은 1이 되고, p가 $8k\pm 3$꼴이면 우변이 -1이 된다. □

정리 3.6 (Gauss, 1801)**.** *서로 다른 홀수 소수 p, q에 대해 다음이 항상 성립한다.*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

사실은 이 정리의 증명도 원시근의 존재성과 마찬가지로 증명을 몰라도 사용할 줄만 알면 올림피아드를 하는데 전혀 지장이 없다. 그래도 아래 증명의 개요를 적어놓았다.

Proof. 집합 $S = \{0 < k < pq : \gcd(k, pq) = 1\}$을 생각하자. S의 다음과 같은 부분집합들을 생각하자.

$$A = \{k \in S : k\text{를 } p\text{로 나눈 나머지는 } p/2\text{보다 작다}\}$$
$$B = \{k \in S : k\text{를 } q\text{로 나눈 나머지는 } q/2\text{보다 작다}\}$$
$$C = \{k \in S : k < pq/2\}$$

이 집합들 A, B, C는 모두 $x \in A \Leftrightarrow pq - x \notin A$와 같은 성질을 가졌다. 따라서 집합들 사이는 x를 $pq - x$로 바꾸는 시행을 함으로써 서로 바꿀 수 있다. 즉, A, B, C의 원소들의 곱을 각각 P_A, P_B, P_C라 하면 P_A, P_B, P_C는 $\bmod pq$로 부호만 다른 관계일 것이다.

우선 A를 $\bmod q$로 보면 각 나머지가 정확히 $(p-1)/2$번씩 등장하므로

$$P_A \equiv (q-1)!^{(p-1)/2} \pmod q$$

임을 알 수 있다. 한편

$$P_C = \frac{(\prod_{i=1}^{q-1} i)(\prod_{i=1}^{q-1} q+i)\cdots(\prod_{i=1}^{q-1}\frac{p-3}{2}q+i)(\prod_{i=1}^{\frac{q-1}{2}}\frac{p-1}{2}q+i)}{p\cdot 2p\cdot\cdots\cdot\frac{q-1}{2}p}$$
$$= \frac{(q-1)!^{(p-1)/2}(\frac{q-1}{2})!}{p^{(q-1)/2}(\frac{q-1}{2})!} = \frac{(q-1)!^{(p-1)/2}}{p^{(q-1)/2}} = \left(\frac{p}{q}\right)P_A \pmod q$$

그러므로 $P_C \equiv (p/q)P_A \pmod{pq}$가 된다. 마찬가지로 $P_C \equiv (q/p)P_B \pmod{pq}$이다.

여기서 A와 B를 비교해보면, A에서 p로 나눈 나머지는 $p/2$보다 작고, q로 나눈 나머지는 $q/2$보다 큰 수들 x를 모두 $pq-x$로 바꿔주면 B가 됨을 알 수 있다. 이 과정에서 부호가 바뀌는 수의 개수는 $(p-1)(q-1)/4$이므로

$$P_A \equiv (-1)^{(p-1)(q-1)/4}P_B \pmod{pq}$$

이 된다. 따라서

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

이다. □

지금까지 얻은 정리들을 모두 다 한 곳에 모아보자.

따름정리 3.7. *홀수 소수 $p < q$와 정수 a, b에 대해 다음이 성립한다.*

(a) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(b) $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p = 4k+1 \\ -1 & \text{if } p = 4k+3 \end{cases}$

(c) $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p = 8k \pm 1 \\ -1 & \text{if } p = 8k \pm 3 \end{cases}$

(d) $\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right)$

이 사실들을 이용하면 임의의 두 p, a에 대해 (a/p)는 기계적으로 구할 수 있다.

예시 3.8. $a = 2016$, $p = 101$로 놓자. 그러면

$$\left(\frac{2016}{101}\right) = \left(\frac{97}{101}\right) = \left(\frac{101}{97}\right) = \left(\frac{4}{97}\right) = \left(\frac{2}{97}\right)^2 = 1$$

이 됨을 쉽게 확인할 수 있다.

이만하면 이론은 충분한 것 같다. 이제 문제를 풀어보며 이차잉여에 관련된 이론을 적용하는 연습을 하자.

연습문제 3.9. (a) 소수 $p = 4k+3$이 $x^2 + y^2$를 나눈다면 $p \mid x, y$임을 보여라. (b) 서로소인 두 정수 x, y에 대해 $x^2 + y^2$의 홀수 소인수는 항상 $4k+1$꼴이어야 함을 증명하여라. 이를 이용하여 $4k+1$꼴의 소수가 무한히 많음을 보여라.

연습문제 3.10 (China TST 1992 3)**.** 임의의 소수 p에 대해, $p \mid x^2 - x + 3$이 정수해를 가질 필요충분조건은 $p \mid y^2 - y + 25$가 정수 해를 가지는 것임을 보여라.

연습문제 3.11. 정수 $n \geq 2$에 대해 페르마 수 $2^{2^n} + 1$의 모든 수인수는 $2^{n+2}k + 1$꼴임을 증명하여라. (연습문제 1.8과 비교해보아라.)

연습문제 3.12. 소수 $p = 4k+1$에 대해, 양의 정수 x, y가 존재하여 $x^2 + y^2 = p$가 됨을 보여라.

연습문제 3.13 (IMO Shortlist 1998 N5)**.** $2^n - 1 \mid m^2 + 9$인 m이 존재하는 양의 정수 n을 모두 구하여라.

연습문제 3.14. 소수 $p = a^2 + 5b^2$이 있고, a는 홀수이다. 이때 a가 mod$p$로 이차잉여일 필요충분조건은 $p \equiv 1 \pmod 5$인 것임을 보여라.

연습문제 3.15. 방정식 $y^2 = x^3 + 23$은 정수근을 갖지 않음을 보여라.

연습문제 3.16. 소수 p와 정수 $p \nmid a, b$에 대해

$$\sum_{i=0}^{p-1} \left(\frac{ai^2 + bi}{p} \right)$$

를 구하여라. 이를 이용해 $ax^2 + bx \equiv y^2 \pmod{p}$의 해 (x, y)의 갯수를 구하여라.

연습문제 3.17 (Romaina TST 2005 12)**.** 실수 x에 대해 $\{x\} = x - \lfloor x \rfloor$을 정의하자. 이때 소수 $p = 8k + 7$과 정수 $n \geq 0$에 대해 다음을 증명하여라.

$$\sum_{k=1}^{p-1} \left\{ \frac{k^{2^n}}{p} - \frac{1}{2} \right\} = \frac{p-1}{2}$$

연습문제 3.18. $2^n - 1 \mid 3^n - 1$인 양의 정수 n을 모두 구하여라.