Algorithmische Zahlentheorie

ICPC-Proseminar-Vortrag vom 22. Mai 2010

Tomáš Přerovský

Abschnitt 1: Grundlagen.

Ringe

Unter einem **Ring** R versteht man eine Menge zusammen mit zwei Operationen $+$ (Addition) und $\times$ (Multiplikation), die folgenden Axiomen genügen:

- $(+, R)$ ist eine abelsche (kommutative) Gruppe mit neutralem Element 0.
- Die Multiplikation ist assoziativ.
- Es gelten die Distributiv-Gesetze :

$$(a+b)c = ac + bc$$

$$c(a+b) = ca + cb$$

Ringe

Unter einem **Ring** R versteht man eine Menge zusammen mit zwei Operationen $+$ (Addition) und $\times$ (Multiplikation), die folgenden Axiomen genügen:

- $(+, R)$ ist eine abelsche (kommutative) Gruppe mit neutralem Element 0.
- Die Multiplikation ist assoziativ.
- Es gelten die Distributiv-Gesetze :

$$(a + b)c = ac + bc$$

$$c(a + b) = ca + cb$$

Ringe

Unter einem **Ring** R versteht man eine Menge zusammen mit zwei Operationen $+$ (Addition) und $\times$ (Multiplikation), die folgenden Axiomen genügen:

- $(+, R)$ ist eine abelsche (kommutative) Gruppe mit neutralem Element 0.
- Die Multiplikation ist assoziativ.
- Es gelten die Distributiv-Gesetze :

$$(a+b)c = ac + bc$$

$$c(a+b) = ca + cb$$

Ringe

Unter einem **Ring** R versteht man eine Menge zusammen mit zwei Operationen $+$ (Addition) und $\times$ (Multiplikation), die folgenden Axiomen genügen:

- $(+, R)$ ist eine abelsche (kommutative) Gruppe mit neutralem Element 0.
- Die Multiplikation ist assoziativ.
- Es gelten die Distributiv-Gesetze :

$$(a+b)c = ac + bc$$

$$c(a+b) = ca + cb$$

Integritätsbereiche

Ein nullteilerfreier kommutativer Ring R mit Einselement heißt **Integritätsring.**Dabei bedeutet

- **Nullteilerfreiheit**, wenn gilt : $x \times y = 0 \Rightarrow x = 0 \vee y = 0$.
- **Kommutativität**, daßdie $\times$ Operation kommutativ ist: $a \times b = b \times a$
- **Einselement**, daßes ein neutrales Element bzgl. der Multiplikation gibt : $\exists e \in R \; \forall x : x \times e = e \times x = x$

Integritätsbereiche

Ein nullteilerfreier kommutativer Ring R mit Einselement heißt **Integritätsring.**Dabei bedeutet

- **Nullteilerfreiheit**, wenn gilt : $x \times y = 0 \Rightarrow x = 0 \vee y = 0$.
- **Kommutativität**, daßdie $\times$ Operation kommutativ ist: $a \times b = b \times a$
- **Einselement**, daßes ein neutrales Element bzgl. der Multiplikation gibt : $\exists e \in R \; \forall x : x \times e = e \times x = x$

Integritätsbereiche

Ein nullteilerfreier kommutativer Ring R mit Einselement heißt **Integritätsring.**Dabei bedeutet

- **Nullteilerfreiheit**, wenn gilt : $x \times y = 0 \Rightarrow x = 0 \vee y = 0$.
- **Kommutativität**, daßdie $\times$ Operation kommutativ ist: $a \times b = b \times a$
- **Einselement**, daßes ein neutrales Element bzgl. der Multiplikation gibt : $\exists e \in R\ \forall x : x \times e = e \times x = x$

Integritätsbereiche

Ein nullteilerfreier kommutativer Ring R mit Einselement heißt **Integritätsring.**Dabei bedeutet

- **Nullteilerfreiheit**, wenn gilt : $x \times y = 0 \Rightarrow x = 0 \vee y = 0$.
- **Kommutativität**, daßdie $\times$ Operation kommutativ ist: $a \times b = b \times a$
- **Einselement**, daßes ein neutrales Element bzgl. der Multiplikation gibt : $\exists e \in R\ \forall x : x \times e = e \times x = x$

Wichtigste Beispiele für Integritätsbereiche

Die wichtigsten Beispiele für Integritätsringe sind :

- Die Menge der ganzen Zahlen $\mathbb{Z}$.
- Der Polynomring in einer Unbestimmten X :

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_2 X^2 + a_1 X + a_0$$

- Der Ring der Gaußschen Zahlen $\mathbb{Z}[i]$:

$$\mathbb{Z}[i] := \{n + im \in \mathbb{C} \ : n, m \in \mathbb{Z}\}$$

Wichtigste Beispiele für Integritätsbereiche

Die wichtigsten Beispiele für Integritätsringe sind :

- Die Menge der ganzen Zahlen $\mathbb{Z}$.
- Der Polynomring in einer Unbestimmten X :

$$a_nX^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + a_1X + a_0$$

- Der Ring der Gaußschen Zahlen $\mathbb{Z}[i]$:

$$\mathbb{Z}[i] := \{n + im \in \mathbb{C} \ : n, m \in \mathbb{Z}\}$$

Wichtigste Beispiele für Integritätsbereiche

Die wichtigsten Beispiele für Integritätsringe sind :

- Die Menge der ganzen Zahlen $\mathbb{Z}$.
- Der Polynomring in einer Unbestimmten X :

$$a_nX^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + a_1X + a_0$$

- Der Ring der Gaußschen Zahlen $\mathbb{Z}[i]$:

$$\mathbb{Z}[i] := \{n + im \in \mathbb{C} \,:\, n, m \in \mathbb{Z}\}$$

Wichtigste Beispiele für Integritätsbereiche

Die wichtigsten Beispiele für Integritätsringe sind :

- Die Menge der ganzen Zahlen $\mathbb{Z}$.
- Der Polynomring in einer Unbestimmten X :

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_2 X^2 + a_1 X + a_0$$

- Der Ring der Gaußschen Zahlen $\mathbb{Z}[i]$:

$$\mathbb{Z}[i] := \{n + im \in \mathbb{C} \; : n, m \in \mathbb{Z}\}$$

Einheiten

Ein Element $u \in R$ heißt **Einheit**, wenn ein $v \in R$ existiert mit $u \times v = 1$. Die Menge aller Einheiten in R wird mit R^* bezeichnet. R^* ist eine multiplikative Gruppe. Zwei Elemente $x, y \in R \setminus \{0\}$ heißen **assoziiert**, falls eine Einheit $u \in R$ existiert mit $x = u \times y$.

Beispiele.

- $\mathbb{Z}^* = \{1, -1\}$
- $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$
- $K[X]^* = K^* = K \setminus \{0\}$

Einheiten

Ein Element $u \in R$ heißt **Einheit**, wenn ein $v \in R$ existiert mit $u \times v = 1$. Die Menge aller Einheiten in R wird mit R^* bezeichnet. R^* ist eine multiplikative Gruppe. Zwei Elemente $x, y \in R \setminus \{0\}$ heißen **assoziiert**, falls eine Einheit $u \in R$ existiert mit $x = u \times y$.

Beispiele.

- $\mathbb{Z}^* = \{1, -1\}$
- $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$
- $K[X]^* = K^* = K \setminus \{0\}$

Einheiten

Ein Element $u \in R$ heißt **Einheit**, wenn ein $v \in R$ existiert mit $u \times v = 1$. Die Menge aller Einheiten in R wird mit R^* bezeichnet. R^* ist eine multiplikative Gruppe. Zwei Elemente $x, y \in R \setminus \{0\}$ heißen **assoziiert**, falls eine Einheit $u \in R$ existiert mit $x = u \times y$.

Beispiele.

- $\mathbb{Z}^* = \{1, -1\}$
- $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$
- $K[X]^* = K^* = K \setminus \{0\}$

Einheiten

Ein Element $u \in R$ heißt **Einheit**, wenn ein $v \in R$ existiert mit $u \times v = 1$. Die Menge aller Einheiten in R wird mit R^* bezeichnet. R^* ist eine multiplikative Gruppe. Zwei Elemente $x, y \in R \setminus \{0\}$ heißen **assoziiert**, falls eine Einheit $u \in R$ existiert mit $x = u \times y$.

Beispiele.

- $\mathbb{Z}^* = \{1, -1\}$
- $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$
- $K[X]^* = K^* = K \setminus \{0\}$

Teilbarkeit

Seien x, y zwei Elemente eines Integritätsbereichs R. Man sagt x teilt y, in Zeichen $x \mid y$, wenn ein $q \in R$ existiert mit $y = qx$.
Gilt nicht $x \mid y$, so schreibt man $x \nmid y$.
Bemerkung. Es gilt stets $x \mid 0$ aber für $y \neq 0$ gilt immer $0 \nmid y$.

Grösster gemeinsamer Teiler

Definition. Seien x, y zwei Elemente eines Integritätsbereichs R. Ein Element $d \in R$ heißt **größter gemeinsamer Teiler** von x und y, falls folgende beiden Bedingungen erfüllt sind:

- $d \mid x$ und $d \mid y$
- Ist $d' \in R$ ein weiteres Element mit $d' \mid x$ und $d' \mid y$, so folgt $d' \mid d$.

Anmerkung.

- Der grösste gemeinsame Teiler ist bis auf Einheiten eindeutig bestimmt, d.h. seien d, d' grösste gemeinsame Teiler von x, y, dann gilt $d = ud'$ mit $u \in R^*$.
- Zwei Elemente $x, y \in R$ heißen teilerfremd, falls 1 grösster gemeinsamer Teiler ist.

Grösster gemeinsamer Teiler

Definition. Seien x, y zwei Elemente eines Integritätsbereichs R. Ein Element $d \in R$ heißt **größter gemeinsamer Teiler** von x und y, falls folgende beiden Bedingungen erfüllt sind:

- $d \mid x$ und $d \mid y$
- Ist $d' \in R$ ein weiteres Element mit $d' \mid x$ und $d' \mid y$, so folgt $d' \mid d$.

Anmerkung.

- Der grösste gemeinsame Teiler ist bis auf Einheiten eindeutig bestimmt, d.h. seien d, d' grösste gemeinsame Teiler von x, y, dann gilt $d = ud'$ mit $u \in R^*$.
- Zwei Elemente $x, y \in R$ heißen teilerfremd, falls 1 grösster gemeinsamer Teiler ist.

Grösster gemeinsamer Teiler

Definition. Seien x, y zwei Elemente eines Integritätsbereichs R. Ein Element $d \in R$ heißt **größter gemeinsamer Teiler** von x und y, falls folgende beiden Bedingungen erfüllt sind:

- $d \mid x$ und $d \mid y$
- Ist $d' \in R$ ein weiteres Element mit $d' \mid x$ und $d' \mid y$, so folgt $d' \mid d$.

Anmerkung.

- Der grösste gemeinsame Teiler ist bis auf Einheiten eindeutig bestimmt, d.h. seien d, d' grösste gemeinsame Teiler von x, y, dann gilt $d = ud'$ mit $u \in R^*$.
- Zwei Elemente $x, y \in R$ heißen teilerfremd, falls 1 grösster gemeinsamer Teiler ist.

Grösster gemeinsamer Teiler

Definition. Seien x, y zwei Elemente eines Integritätsbereichs R. Ein Element $d \in R$ heißt **größter gemeinsamer Teiler** von x und y, falls folgende beiden Bedingungen erfüllt sind:

- $d \mid x$ und $d \mid y$
- Ist $d' \in R$ ein weiteres Element mit $d' \mid x$ und $d' \mid y$, so folgt $d' \mid d$.

Anmerkung.

- Der grösste gemeinsame Teiler ist bis auf Einheiten eindeutig bestimmt, d.h. seien d, d' grösste gemeinsame Teiler von x, y, dann gilt $d = ud'$ mit $u \in R^*$.
- Zwei Elemente $x, y \in R$ heißen teilerfremd, falls 1 grösster gemeinsamer Teiler ist.

Euklidischer Ring

Definition. Ein Integritätsbereich R heißt **euklidischer Ring**, falls es eine Funktion $\beta : R \to \mathbb{N}$ gibt, so daß folgendes gilt : Für je zwei Elemente $x, y \in R, y \neq 0$, existiert eine Darstellung

$$x = qy + r, \quad q, r \in R$$

wobei $r = 0$ oder $\beta(r) < \beta(y)$.

Die wichtigsten Beispiele für euklidische Ringe

Satz.[1] Die Ringe $\mathbb{Z}, \mathbb{Z}[i]$ und $K[X]$ für einen beliebigen Körper K sind euklidisch.

- Für $\mathbb{Z}$ definiere $\beta(x) :=\mid x \mid$
- Für $\mathbb{Z}[i]$ definiere $\beta(x_1 + ix_2) := x_1^2 + x_2^2$
- Im Polynomring $K[x]$ definiere $\beta(P) := deg(P)$ als den Grad des Polynoms. Dabei ist der Grad von $P(X) = \sum_{i=0}^{n} a_i X^i$ der höchste Koeffizient $\neq 0$. Der Grad des Null-Polynoms ist 0.

[1] Beweis findet sich in der Ausarbeitung zu diesem Vortrag.

Hauptsatz über euklidische Ringe

Nun kommen wir zum **Hauptsatz** über euklidische Ringe.

Satz. In einem euklidischen Ring R besitzen je zwei Elemente $x, y \in R$ einen grössten gemeinsamen Teiler.

Beweis des Hauptsatzes über euklidische Ringe

Beweis. Falls $y = 0$, ist x ein größter gemeinsamer Teiler. ObdA sei $y \neq 0$. Sei $\beta : R \to \mathbb{N}$ die Betragsfunktion. Der Beweis erfolgt durch vollständige Induktion über die natürliche Zahl $\beta(y)$.

Induktionsanfang $\beta(y) = 0$.

Dann bleibt bei der Division von x durch y kein Rest, also ist y größter gemeinsamer Teiler.

Induktionsschritt. Division mit Rest liefert:

$$x = qy + r, \quad \text{wobei } r = 0 \text{ oder } \beta(r) < \beta(y). \tag{1}$$

Falls $r = 0$ ist y größter gemeinsamer Teiler. Andernfalls können wir die Induktionsvoraussetzung auf y, r anwenden. Sei d größter gemeinsamer Teiler von y und r. Dann gilt $d \mid x$ und $d \mid y$. Zudem folgt aus $d' \mid x$ und $d' \mid y$, daß $d' \mid r$, also aufgrund der Definition von d auch $d' \mid d$. **q.e.d.**

$gcd(x, y)$

Für ganze Zahlen x, y ist der größte gemeinsame Teiler bis auf einen Faktor ± 1 eindeutig bestimmt. Den eindeutig bestimmten nicht-negativen größten gemeinsamen Teiler bezeichnen wir mit $gcd(x, y)$ (von engl. *greatest common divisior*).

Die Idee des Beweises ist sehr einfach : Führe die Berechnung von $gcd(x, y)$ auf die von $gcd(y, x \bmod y)$ zurück.
Beispiel:
$gcd(100, 35) = gcd(35, 100 \bmod 35) = gcd(35, 30) = gcd(30, 5) = gcd(5, 0) = 5.$

Erste Version des Euklidischen Algorithmus

Der Beweis des Hauptsatzes liefert unmittelbar einen Algorithmus zur Bestimmung des größten gemeinsamen Teilers, den vor über 2000 Jahren gefundenen *euklidischen Algorithmus* (in C++):

```
template <typename T> T gcd (const T& x, const T& y)
{
   if (y == T())
      return abs(x);
   else
      return gcd(y, x % y);
}
```

Worst Case Laufzeit: im Falle zweier benachbarter Fibonacci-Zahlen

Der euklidische Algorithmus benötigt für zwei benachbarte Fibonacci-Zahlen F_n, F_{n+1} aufgrund der Identität

$$F_{n+1} = 1 \cdot F_n + F_{n-1}$$

n Divisionen mit Rest. Eine einfache Überlegung[2], zeigt dass dies gleichzeitig auch die maximale Anzahl von Divisionen für x, y mit $x, y \leq F_{n+1}$ ist. Da $F_n = \frac{1}{\sqrt{5}}\left(g^n - \frac{(-1)^n}{g^n}\right)$ ist, wobei $g := \frac{1}{2}(1+\sqrt{5})$ der goldene Schnitt ist. Ist die worstcase Komplexität des euklidischen Algorithmus $O(\log n)$.

[2] Details entnehme man z.B. [Fo] Seite 26

Bevor's weiter geht: nichtrekursive Version des euklidischen Algorithmus

```
template <typename T> T gcd_it (const T& x, const T& y)
{
    T temp,y_=y,x_=x;
    for(;y_ != T() ;)
    {
        temp = y_;
        y_ = x_ % y_;
        x_ = temp;
    }
    return abs(x_);
}
```

Abschnitt 2: Der erweiterte euklidische Algorithmus.

Wir können nun den *gcd* zweier Zahlen berechnen, aber die folgende Aufgabe fordert mehr !

PC/UVa IDs: 110703/10104, **Popularity:** A, **Success rate:** average **Level:** 1

From Euclid, it is known that for any positive integers A and B there exist such integers X and Y that $AX + BY = D$, where D is the greatest common divisor of A and B. The problem is to find the corresponding X, Y, and D for a given A and B.

Input

The input will consist of a set of lines with the integer numbers A and B, separated with space ($A, B < 1{,}000{,}000{,}001$).

Output

For each input line the output line should consist of three integers X, Y, and D, separated with space. If there are several such X and Y, you should output that pair for which $X \leq Y$ and $|X| + |Y|$ is minimal.

Sample Input

```
4 6
17 17
```

Sample Output

```
-1 1 2
0 1 17
```

Zurück zur Theorie: Ideale

Definition. Eine Teilmenge $I \subset R$ eines kommutativen Ringes R heisst **Ideal**, wenn gilt:

- I ist eine additive Unterruppe von R, d.h. I ist nicht leer und

$$x, y \in I \Rightarrow x + y \in I \wedge -x \in I$$

- Für alle $\lambda \in R$ und $x \in I$ gilt $\lambda x \in I$

Zurück zur Theorie: Ideale

Definition. Eine Teilmenge $I \subset R$ eines kommutativen Ringes R heisst **Ideal**, wenn gilt:

- I ist eine additive Unterruppe von R, d.h. I ist nicht leer und

$$x, y \in I \Rightarrow x + y \in I \wedge -x \in I$$

- Für alle $\lambda \in R$ und $x \in I$ gilt $\lambda x \in I$

Zurück zur Theorie: Ideale

Definition. Eine Teilmenge $I \subset R$ eines kommutativen Ringes R heisst **Ideal**, wenn gilt:

- I ist eine additive Unterruppe von R, d.h. I ist nicht leer und

$$x, y \in I \Rightarrow x + y \in I \wedge -x \in I$$

- Für alle $\lambda \in R$ und $x \in I$ gilt $\lambda x \in I$

Beispiele

- Für ein beliebiges Element $x \in R$ ist
$$Rx = \{\lambda x : \lambda \in R\}$$
ein Ideal. Es ist das kleinste Ideal von R, das x enthält und heißt das von x erzeugte **Hauptideal** und wird mit (x) bezeichnet.
- Allgemeiner : seien $x_1, \cdots, x_r \in R$. Dann ist
$$Rx_1 + \cdots + Rx_r = \{\lambda x_1 + \cdots + \lambda x_r : \lambda_1, \ldots, \lambda_r \in R\}$$
ebenfalls ein Ideal, das von $x_1, \ldots, x_r$ erzeugte Ideal. Es wird mit $(x_1, \cdots, x_r)$ bezeichnet.

Beispiele

- Für ein beliebiges Element $x \in R$ ist

$$Rx = \{\lambda x : \lambda \in R\}$$

ein Ideal. Es ist das kleinste Ideal von R, das x enthält und heißt das von x erzeugte **Hauptideal** und wird mit (x) bezeichnet.

- Allgemeiner : seien $x_1, \cdots, x_r \in R$. Dann ist

$$Rx_1 + \cdots + Rx_r = \{\lambda x_1 + \cdots + \lambda x_r : \lambda_1, \ldots, \lambda_r \in R\}$$

ebenfalls ein Ideal, das von $x_1, \ldots, x_r$ erzeugte Ideal. Es wird mit $(x_1, \cdots, x_r)$ bezeichnet.

Beispiele

- Für ein beliebiges Element $x \in R$ ist

$$Rx = \{\lambda x : \lambda \in R\}$$

  ein Ideal. Es ist das kleinste Ideal von R, das x enthält und heißt das von x erzeugte **Hauptideal** und wird mit (x) bezeichnet.
- Allgemeiner : seien $x_1, \cdots, x_r \in R$. Dann ist

$$Rx_1 + \cdots + Rx_r = \{\lambda x_1 + \cdots + \lambda x_r : \lambda_1, \ldots, \lambda_r \in R\}$$

  ebenfalls ein Ideal, das von $x_1, \ldots, x_r$ erzeugte Ideal. Es wird mit $(x_1, \cdots, x_r)$ bezeichnet.

Euklidische Ringe sind Hauptidealringe

Satz. Sei R ein Integritätsbereich. Dann gilt für $x, y \in R$

$$x \mid y \iff (y) \subset (x)$$

Beweis. ´$\Rightarrow$´ Aus $x \mid y$ folgt $y = qx$ für ein geeignetes $q \in R$, also $\lambda y = \lambda qx \in (x) \forall \lambda \in R$, d.h. $(y) \subset (x)$.
$\Leftarrow$. Aus $(y) \subset (x)$ folgt $y \in (x)$, d.h. $y = \lambda x$ mit $\lambda \in R$. Das bedeutet aber $x \mid y$

Euklidische Ringe sind Hauptidealringe

Corollar. Seien $x_1, \ldots, x_r \in R$ Elemente eines Integritätsbereichs R. Ein Element $d \in R$ ist genau dann gemeinsamer Teiler der x_i, d.h. $d \mid x_i$ für alle $i = 1, \ldots, r$, wenn

$$(x_1, \ldots, x_r) \subset (d)$$

Euklidische Ringe sind Hauptidealringe

Definition. Ein Integritätsbereich R heisst **Hauptidealring**, wenn jedes Ideal $I \subset R$ ein Hauptideal ist, d.h. ein $d \in R$ existiert mit $I = (d)$.

Euklidische Ringe sind Hauptidealringe

Es gilt nun der wichtige
Satz. *Jeder euklidische Ring ist ein Hauptidealring.*
Beweis Siehe Ausarbeitung.

Euklidische Ringe sind Hauptidealringe

Corollar. Seien $x_1, \ldots, x_r$ Elemente eines Hauptidealrings R und d ein größter gemeinsamer Teiler der x_i. Dann gibt es Elemente $\lambda_1, \ldots, \lambda_r \in R$ mit

$$d = \lambda_1 x_1 + \ldots + \lambda_r x_r$$

Der erweiterte euklidische Algorithmus

Es wird solange mit Rest geteilt,

$$x_{i-1} = q_i x_i + x_{i+1}, \quad i = 1, \dots, n$$

bis der Rest 0 bleibt, d.h. $x_{n+1} = 0$ aber $x_n = 0$. Schreibt man dies in Matrizenform lässt sich dies wie folgt ausdrücken:

$$\begin{pmatrix} x_i \\ x_{i+1} \end{pmatrix} = Q_i \begin{pmatrix} x_{i-1} \\ x_i \end{pmatrix}, \text{wobei} Q_i = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$$

Der erweiterte euklidische Algorithmus

Daraus erhält man dann:

$$\begin{pmatrix} x_i \\ x_{i+1} \end{pmatrix} = Q_n \cdot Q_{n-1} \cdot \dots \cdot Q_1 \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}.$$

Der erweiterte euklidische Algorithmus

Man muss also nur sukzessive die Matrizen

$$\Delta_0 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \Delta_i := \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \Delta_{i-1}$$

ausrechnen.

Der erweiterte euklidische Algorithmus : C++ Code

```
template <typename T> void gcd_coeff(T x,T y,T& res_gcd, T& res_coeff1, T& res_coeff2)
{
    T q,temp,q11,q12,q21,q22,t21,t22;
    q11 = q22 = 1;
    q12 = q21 = 0;
    for(;y!=T();)
    {
        temp = y;
        q = x / y;
        y = x % y;
        x = temp;
        t21 = q21;t22 = q22;
        q21 = q11 - q*q21;
        q22 = q12 - q*q22;
        q11 = t21; q12 = t22;
    }
    res_gcd = x;
    res_coeff1 = q11;
    res_coeff2 = q12;
}
```

Abschnitt 3: Der Restklassenring $\mathbb{Z}/m\mathbb{Z}$.

Definition von $x \equiv y \mod m\mathbb{Z}$

Definition. Sei m eine ganze Zahl. Betrachte das Hauptideal $m\mathbb{Z} \subset \mathbb{Z}$ und führe folgende **Äquivalenzrelation** ein: Zwei Zahlen $x, y \in \mathbb{Z}$ heißen äquivalent modulo m, oder auch kongruent modulo m in Zeichen

$$x \equiv y \mod m\mathbb{Z},$$

wenn $x - y \in \gtrdot\mathbb{Z}$

Einfache Tatsachen zu $\mathbb{Z}/m\mathbb{Z}$

Für $m = 0, 1$ haben wir die Trivialfälle der Identität bzw. der Relation $\mathbb{Z} \times \mathbb{Z}$. Im Falle $m \geq 2$ sind zwei Zahlen x, y genau dann äquivalent $\mod m$, wenn sie bei Division durch m denselben Rest $r \in \{0, 1, \ldots, m-1\}$ lassen. Die Menge

$$\{0, 1, \ldots, m-1\}$$

stellt deshalb ein vollständiges Repräsentantensystem für die Äquivalenzklassen $\mod m\mathbb{Z}$ dar und daher hat $\mathbb{Z}/m\mathbb{Z}$ genau m Elemente. Die Äquivalenzklasse einer Zahl x wird mit $x \mod m$, $[x]$ oder $\bar{x}$ bezeichnet. Damit schreibt man :

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}.$$

$\mathbb{Z}/m\mathbb{Z}$ ist ein Ring

Definition. Auf $\mathbb{Z}/m\mathbb{Z}$ wird eine Addition und eine Multiplikation erklärt:

$$\overline{x} + \overline{y} := \overline{x + y}$$

$$\overline{x} \cdot \overline{y} := \overline{x \cdot y}$$

Die Ringaxiome für die Addition und Multiplikation vererben sich auf $\mathbb{Z}/m\mathbb{Z}$, so dass $\mathbb{Z}/m\mathbb{Z}$ wiederum ein kommutativer Ring mit Einselement ist.

Beispiel

Im Ring $\mathbb{Z}/5\mathbb{Z}$ gilt

$$\overline{2} + \overline{3} = \overline{5} = \overline{0}$$

und

$$\overline{2} \cdot \overline{3} = \overline{6} = \overline{1}$$

also gilt in $\mathbb{Z}/5\mathbb{Z}$: $-\overline{2} = \overline{3}$ und $\overline{2}^{-1} = \overline{3}$

$\phi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}$ ist ein Ring-Homomorphismus

Definiert man die Abbildung $\phi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}$ vermittels $\phi(x) := \overline{x}$ so ist ϕ ein sogenannter Ringhomomorphismus. Die Eigenschaften dieses Homomorphismus sind explizit oder implizit Gegenstand zahlreicher ICPC - Aufgaben.

Beispiel

PC/UVa IDs: 110704/10139, **Popularity:** A, **Success rate:** average **Level:** 2

The factorial function, $n!$ is defined as follows for all non-negative integers n:

$$\begin{aligned} 0! &= 1 \\ n! &= n \times (n-1)! \qquad (n > 0) \end{aligned}$$

We say that a divides b if there exists an integer k such that

$$k \times a = b$$

Input

The input to your program consists of several lines, each containing two non-negative integers, n and m, both less than 2^{31}.

Output

For each input line, output a line stating whether or not m divides $n!$, in the format shown below.

Sample Input

```
6 9
6 27
20 10000
20 100000
1000 1009
```

Sample Output

```
9 divides 6!
```

Wann ist ein Element x in $\mathbb{Z}/m\mathbb{Z}$ invertierbar ?

Satz. Die Restklasse $x \mod m$ ist im Ring $\mathbb{Z}/m\mathbb{Z}$ genau dann invertierbar, wenn $gcd(x, m) = 1$ also x und m relativ prim sind.
Beweis. Einfache Anwendung des erweiterten euklidischen Algorithmus.

Wann ist $\mathbb{Z}/m\mathbb{Z}$ sogar ein Körper ?

Corollar Für jede Primzahl p ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper.

Chinesischer Restsatz : Vorbemerkung

Wir kommen nun zum sog. Chinesischen Restsatz. Der vorallem wegen seiner theoretischen Bedeutung eine tragende Rolle im Aufbau der algebraischen Zahlentheorie spielt. Zuerst aber eine

Definition. Seien $A_1, \ldots, A_r$ Ringe. Unter dem direkten Produkt der Ringe $A_1, \ldots, A_r$ versteht man die Menge

$$A := A_1 \times \ldots \times A_r$$

mit der komponentenweise erklärten Addition bzw. Multiplikation ist A ein Ring.

Chinesischer Restsatz

Chinesischer Restsatz. Sei $m > 1$ eine natürliche Zahl und

$$m = m_1 \cdot m_2 \cdots m_r$$

eine Zerlegung von m in paarweise teilerfremde Zahlen $m_i > 1$. Dann ist die kanonische Abbildung

$$\Phi : \mathbb{Z}/m\mathbb{Z} \to (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_r\mathbb{Z}),$$

$$x \mod m \mapsto (x \mod m_1, \ldots, y \mod m_r)$$

ein Ring-**Iso**morphismus.

Zuerst eine theoretische Anwendung

Bevor wir uns dem Beweis und damit der genauen Struktur der Abbildung Φ zuwenden, soll anhand eines prominenten Beispiels die theoretische Durchschlagskraft demonstriert werden.

Euler's φ-Funktion

Für eine natürliche Zahl $m > 1$ bezeichne $\varphi(m)$ die Anzahl der zu m teiler**fremden** Zahlen $< m$. Wir suchen nun nach einer geschlossenen Darstellung dieser Funktion, und können bei dieser Gelegenheit die Mächtigkeit der bisher eingeführten Begriffe demonstrieren.

1. Schritt : Abbilden des Problems in die Sprache der Restklassen

Welche Menge hat dieselbe Anzahl wie die Menge der zu m teilerfremden Zahlen $< m$?

$(\mathbb{Z}/m\mathbb{Z})^*$!

Es gilt :

$$\varphi(m) = Card((\mathbb{Z}/m\mathbb{Z})^*).$$

2. Schritt : Anwendung der Primfaktorzerlegung

Sei $p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ die Primfaktorzerlegung von m.

3. Schritt : Nun können wir den chinesischen Restsatz anwenden

Es gilt ja $\mathbb{Z}/m\mathbb{Z} \cong (\mathbb{Z}/p_1^{k_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_r^{k_r}\mathbb{Z})$
und damit auch $(\mathbb{Z}/m\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_r^{k_r}\mathbb{Z})^*$

$\varphi(m) = \prod Card((\mathbb{Z}/p_i^{k_i})^*)$

Also ist $\varphi(m) = Card((\mathbb{Z}/m\mathbb{Z})^*) = \prod Card((\mathbb{Z}/p_i^{k_i}\mathbb{Z})^*)$

$Card((\mathbb{Z}/p_i^{k_i}\mathbb{Z})^*)$?

Was ist aber $Card((\mathbb{Z}/p_i^{k_i}\mathbb{Z})^*)$? D.h. die Anzahl der Zahlen in $\{0, 1, \ldots, p^k - 1\}$ die teilerfremd sind zu $p_i^{k_i}$?

Da p prim ist sind unter den Zahlen $\{0, \ldots, p^k - 1\}$ nur genau die Vielfachen von p nicht teilerfremd. Somit ist

$$Card((\mathbb{Z}/p_i^{k_i}\mathbb{Z})^*) = p^{k_i} - p^{k_i - 1}$$

und wir erhalten den Satz:

$$\varphi(m) = \prod_{i=1}^{r}(p_i^{k_i} - p_i^{k_i - 1}) = m\prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)$$

Zurück zum Chinesischen Restsatz

Dass Φ ein (Ring-)Homomorphismus ist, ist klar. Wir interessieren uns also dafür ob Φ bijektiv ist, insbesondere interessiert uns die explizite Angabe des Urbilds von $a \in Bild\{\Phi\}$. Können wir nebenbei zeigen, dass Φ surjektiv ist fällt uns die Injektivität und damit die Bijektivität automatisch in die Hände (Warum ?).

Was ist das Urbild von $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$?

Wir müssen eine ganze Zahl u_i finden, so dass

$$u_i \equiv 1 \mod m_i \text{ und} \tag{2}$$
$$u_i \equiv 0 \mod m_k \text{ für } k \neq i \tag{3}$$

Sei $z_i := \prod_{k \neq i} m_k = m/m_i$. Dann ist $z_i \equiv 0 \mod m_k$ für alle $k \neq i$. Außerdem sind z_i und m_i teilerfremd, demnach gibt es eine ganze Zahl y_i mit $z_i y_i \equiv 1 \mod m_i$. Die Zahl $u_i := z_i y_i$ erfüllt die geforderten Bedingungen. Sind nun x_i beliebige ganze Zahlen, so gilt für $x = \sum_{i=1}^{r} x_i u_i$:

$$x \equiv x_i \mod m_i \ \forall i = 1, \ldots, r.$$

Damit ist die Surjektivität von Φ gezeigt.

Weiterführende Literatur I

Michael Artin.
Algebra.
Prentice-Hall, 1991.

Otto Forster.
Algorithmische Zahlentheorie.
Vieweg, 1996.

Thomas H Cormen, et al.
Introduction to Algorithms.
MIT Press, 2009.

Johannes Buchmann.
Einführung in die Kryptographie.
Springer Verlag, 2003.

Weiterführende Literatur II

Ronald L. Graham, Donald E. Knuth, Oren Patashnik.
Concrete Mathematics.
Addison-Wesley, 1994.