ФЕРМАОВ ПОСТУПАК РАСТАВЉАЊА ПРИРОДНОГ БРОЈА НА ЧИНИОЦЕ

Ђура Паунић, Нови Сад

У програмирању математичких израза се често јавља потреба за генерисањем низа квадрата

$$1,\ 4,\ 9,\ 16,\ \ldots,\ n^2,\ldots$$

при чему овај низ не мора да почне јединицом. Овај низ се једноставно прогамира `for` петљом:

```
for i := 1 to n do
  begin
    kvadrat := sqr(i);
    write(kvadrat : 4)
  end;
writeln;
```

Међутим, сабирање два цела броја је брже од множења два цела броја, па је могуће ову једноставну петљу убрзати на следећи начин. Испишимо испод свака два суседна квадрата њихову разлику. Добија се низ

$$\begin{array}{ccccccccccc} 1, & & 4, & & 9, & & 16, & & 25, & \ldots \\ & 3, & & 5, & & 7, & & 9, & & \ldots. \end{array}$$

Низ разлика је аритметичка прогресија, па се низ квадрата може добити тако да се на почетну јединицу у сваком кораку додаје члан аритметичке прогресије чији је почетни члан 3, а разлика 2. То се реализује следећим програмским фрагментом.

```
sabirak := 1;
kvadrat := 1;
write(kvadrat : 4);
for i := 1 to n-1 do
  begin
    sabirak := sabirak + 2;
    kvadrat := kvadrat + sabirak;
    write(kvadrat : 4)
  end;
writeln;
```

Интересантно је да је овај једноставан поступак генерисања квадрата искористио велики француски математичар Пјер Ферма (Pierre Fermat, 1601 – 1665) за поступак факторизације природних бројева у коме се не користи дељење. Наиме, уобичајени поступак за разлагање природног броја n на просте чиниоце је да се n дели простим бројевима који су мањи од $\sqrt{n}$. Од свих аритметичких операција дељење је најкомпликованије, па се Ферма запитао да ли је могуће пронаћи поступак факторизације који не користи дељење. Тако је успео да нађе поступак факторизације који не користи ни дељење ни множење.

Фермаова метода факторизације се заснива на једноставној чињеници да се сложен непаран број може приказати као разлика два квадрата:

Тврђење. *Нека је n непаран природан број. Тада постоји бијекција између свих факторизација броја $n = pq$, $p \geq q > 0$, и свих репрезентација броја $n = a^2 - b^2$, $a \geq b > 0$.*

Дакле, проблем факторизације се своди на налажење два квадрата тако да је n њихова разлика.

Најпре треба узастопно делити n са два док се не добије непаран број и проверити да ли је n потпун квадрат, што не претставља тешкоће.

Затим се прави низ: $n_0 = k^2 - n$, $n_1 = (k+1)^2 - n$, ..., $n_i = (k+i)^2 - n$, ... где је k први цео број већи од $\sqrt{n}$, $(k-1)^2 < n < k^2$. Када се у низу $\{n_i\}$ појави потпун квадрат, нека је то $n_j = s^2$, тада је $n = (k+j)^2 - s^2 = (k+j+s)(k+j-s)$.

Израчунавање елемената низа $\{n_i\}$ је врло једноставно, јер се бројеви лако добијају рекурзивно са $n_{i+1} = n_i + 2(k+i) + 1$, тј. нов број се добија додавањем разлике на стари, а разлика се у сваком кораку повећава за 2. То је поступак генерисања квадрата који је управо описан.

Ако се факторизација ради ручно, тада је Ферма лако препознавао да ли је n_i квадрат, јер се квадрат мора завршавати цифром 0, 1, 4, 5, 6 и 9, или ако се посматрају задње две цифре, тада су могући само парови цифара:

$$00,\ 01,\ 04,\ 09,\ 16,\ 21,\ 24,\ 25,\ 29,\ 36,\ 41,$$

$$44,\ 49,\ 56,\ 61,\ 64,\ 69,\ 76,\ 81,\ 84,\ 89,\ 96.$$

Они могу једноставније да се запишу са

$$00,\ e1,\ e4,\ 25,\ o6,\ e9,$$

где је са e означена парна цифра, а са o непарна.

Мало модификовани Фермаов поступак може лако да се испрограмира.

– Најпре се издвоји степен двојке тако да остане непаран број.

– Затим се провери да ли је n потпун квадрат и ако јесте поступак се завршава.

– Нека је $n = pq$, $p > q$, непаран број,

$$n = a^2 - b^2, \quad a = \frac{p+q}{2}, \quad b = \frac{p-q}{2}, \quad n \geq a > b \geq 0.$$

Ако n није потпун квадрат тада је $(k-1)^2 < n < k^2$ за неки природан број k, па је $r = k^2 - n > 0$. Сада почињемо да одузимамо квадрате:

$$k^2 - 1 - n, \quad k^2 - 4 - n, \quad k^2 - 9 - n, \text{ итд.}$$

Нека се после извесног броја корака добије да је $r = a^2 - b^2 - n$, разлика између разлике квадрата и броја n. Ако је r нула тада је $n = a^2 - b^2 = (a-b)(a+b)$, факторизација је нађена и поступак се завршава. Ако је r различито од нуле тада су могућа два случаја: или је $r > 0$ када треба повећати b^2 на следећи већи квадрат, или је $r < 0$, а тада треба повећати a^2 на следећи већи квадрат.

Означимо са $\lfloor t \rfloor$ највећи цео број који није већи од реалног броја t. Иницијализујмо r са $\lfloor \sqrt{n} \rfloor^2 - n$, а у x ставимо разлику за коју се повећава a, тј. $2\lfloor \sqrt{n} \rfloor - 1$, јер се корак прво повећава за 2, а тек тада додаје на r. Аналогно је у y почетна вредност за b, $y = -1$, умањена за 2, јер се y најпре повећава за 2, па тек онда одузима од r. Петља се завршава када је $r = 0$, тј. када је нађена факторизација, нетривијална или тривијална. Тада је $x = 2(a-1) + 1 = 2a - 1$, а $y = 2(b-1) + 1 = 2b - 1$, па је $p = a + b = (x + y + 2)/2$ и $q = a - b = (x - y)/2$.

Овим поступком се у општем случају не добија потпуна факторизација броја n на просте чиниоце, него се налазе степен двојке и два непарна чиниоца.

```
procedure fermat(n : integer);

var
  pom, x, y, r : integer;

begin
  while not odd(n) do
    begin
      write(2:5);
      n := n div 2
    end;
  pom := trunc(sqrt(n));
  r := sqr(pom) - n;
  x := 2*pom - 1;
  y := - 1;
  while r <> 0 do
```

```
    begin
      while r < 0 do
        begin
          x := x + 2;
          r := r + x
        end;
      y := y + 2;
      r := r - y
    end;
  pom := (x - y) div 2;
  write(pom:5, n div pom:5)
end; (* fermat *)
```

Предност Фермаовог поступка је да не користи дељење, али дужина петље може да буде много већа него при дељењу броја n простим бројевима који су мањи од $\sqrt{n}$ када је њена дужина, у најгорем случају, реда $\sqrt{n}$. Број корака у Фермаовом поступку је очигледно пропорционалан $p - \lfloor\sqrt{n}\rfloor$, где је p већи чинилац, тако да ако је p много веће од q (на пример q реда $n^{1/4}$, а p реда $n^{3/4}$) тада се добија да је дужина петље реда $n^{3/4}$, што је много веће од $\sqrt{n}$. За велике бројеве n не треба користити Фермаову факторизацију уколико нисмо сигурни да је n сложен број, јер ако је n прост број тада је дужина петље једнака половини броја n.

Фермаов метод факторизације је веома погодан ако се унапред зна да је приближан однос чинилаца број r, $p \approx rq$. Тада је $n = pq \approx rq^2$, па је у том случају $rn \approx (rq)^2$ и rn се може успешно факторисати.

Пример: За факторизацију броја 141467 Фермаовим поступком је погодно факторисати $3n$, тј. почети са $k = \lfloor\sqrt{3n}\rfloor + 1 = 652$, јер се убрзо (из четвртог покушаја) добија да је $655^2 - 3 \cdot 141467 = 68^2$. Израчунавајући $\mathrm{NZD}(655 + 68, 141467) = 241$ добија се да је $141467 = 241 \cdot 587$. Ако се пође од $k = \lfloor\sqrt{141467}\rfloor = 377$, факторизација се добија тек кроз 38 корака.

Задаци

1. Доказати тврђење у чланку.
2. Направити поступак генерисања низа кубова природних бројева у коме се не користи множење.
3. Процедура `fermat` не даје увек разлагање природног броја n на просте чиниоце. Написати програм у коме се овај поступак понавља више пута док се не добије факторизација броја n на просте чиниоце.

Статијата прв пат е објавена во списанието Тангента на ДМ на Србија во 1996/97 година