Факторизация полиномов: Линейный подъем по Гензелю:

$$Z_p \to Z_{p^2} \to Z_{p^3} \to ... \to Z_{p^n} \to Z$$

$SPACE = Z[x];$

ЗАДАЧА

Требуется найти два полинома с целыми коэффициентами, произведение которых равно
$f = x^6 + 25x^5 + 38x^4 + 977x^3 + 350x^2 + 494x + 182.$

Если известно, что образ полинома f при отображении $Z - - > Z_p$ в простое поле по модулю $p = 11$, будет полином
$F_0 = x^6 + 3x^5 + 5x^4 + 9x^3 + 9x^2 - x + 6,$
который раскладывается в $Z_p[x]$ на взаимно простые множители со старшими коэффициентами 1:
$a_0 = x^3 + 3x^2 + 2; b_0 = x^3 + 5x + 3$

Проверим это:
$c_0 = a_0 b_0; c_{map} = \mathbf{mod}(c_0, 11); f_{map} = \mathbf{mod}(f, 11); sub = \mathbf{mod}(f - F_0, 11); \quad \mathbf{print}(c_0, c_{map}, f_{map}, sub);$
$out:$

$c_0 = x^6 + 3x^5 + 5x^4 + 20x^3 + 9x^2 + 10x + 6$
$c_{map} = x^6 + 3x^5 + 5x^4 - 2x^3 - 2x^2 - x - 5$
$f_{map} = x^6 + 3x^5 + 5x^4 - 2x^3 - 2x^2 - x - 5$
$sub = 0$

ОТСУПЛЕНИЕ о том как подбирались эти входные данные.

Были выбраны два случайных полинома
$t1 = (x^3 + 25x^2 + 13); t2 = x^3 + 38x + 14;$

Найдено их произведение
$f = t1 \cdot \ t2;$
$out:$

$x^6 + 25x^5 + 38x^4 + 977x^3 + 350x^2 + 494x + 182$

ПРОДОЛЖЕНИЕ ОТСУПЛЕНИЯ.

Выбрано конечное поле и кольцо полиномов над ним:
$SPACE = Zp32[x]; MOD32 = 11;$

Отобразили полиномы в это кольцо и взяли как входные данные:
$t1p = \mathbf{toNewRing}(t1); t2p = \mathbf{toNewRing}(t2); tFp = (t1p \cdot t2p);$
$\mathbf{print}(t1p, t2p, tFp)$
$out:$

$t1p = x^3 + 3x^2 + 2$
$t2p = x^3 + 5x + 3$
$tFp = x^6 + 3x^5 + 5x^4 + 9x^3 + 9x^2 - x + 6$

РЕШЕНИЕ

Пусть каждый коэффициент полинома записан, как целое число по основанию p.

Тогда

$$f = f_0 + pf_1 + p^2 f_2 + p^3 f_3, \qquad (0)$$

где каждое слагаемое - это полином с коэффициентами, которые лежат в интервале [0,..,p-1], но еще имеют знак и домножены на степень числа p.

Устроим «лифт» по степеням p и будем поднимать решение последовательно до

$Z/(p^2)Z$, $Z/(p^3)Z$, и так далее.

(1) Пусть pa_1 и pb_1 искомые добавки к a_0 и b_0, такие, что

$$(a_0 + pa_1)(b_0 + pb_1) = \mathbf{mod}(f, p^2) = f_0 + pf_1 \qquad (1)$$

Тогда по модулю p^2 верно равенство:
$SPACE = Z[x]; pf_1 = p(a_0b_1 + b_0a_1) = (f - a_0b_0)$
$f_1 = a_0\ b_1 + b_0\ a_1 = (f - a_0b_0)/p;$
$out:$

$2x^5 + 3x^4 + 87x^3 + 31x^2 + 44x + 16$

Задача свелась к нахождению неизвестных сомножителей b_1 и a_1 в Евклидовом кольце $Z_p[x]$ в равенстве

$$a_0b_1 + b_0a_1 = f_1. \qquad (2)$$

Если b_1 и a_1 – некоторое решение, то прибавление к ним любого полинома, который кратен p, не влияет на равенство (1), так как эта добавка по модулю p^2 равна 0.

Так как a_0 и b_0 взаимно просты, то $\mathbf{extandedGCD}(a_0, b_0)$ вернет полиномы A и B, такие, что

$$Aa_0 + Bb_0 = 1.$$

Найдем их:

$SPACE = Zp32[x]; MOD32 = 11; a_{p0} = \mathbf{toNewRing}(a_0); b_{p0} = \mathbf{toNewRing}(b_0); f_{p1} = \mathbf{toNewRing}(f_1);$
$VP = \mathbf{extendedGCD}(a_{p0}, b_{p0}); VP = (vp_i); A_p = vp_2; B_p = vp_3;$
$gcd = \ A_pa_{p0} + B_pb_{p0};$
$\mathbf{print}(A_p, B_p, gcd);$
$out:$

$A_p = -2x^2 - 5x + 3$
$B_p = 2x^2 + 2$
$gcd = 1$

Следовательно, частным решением будет

$$b_{p1} = A_pf_{p1},$$
$$a_{p1} = B_pf_{p1}.$$

Так как общим решением, соответствующего (2) однородного уравнения, будет $(qb_{p0}, -qa_{p0})$, где q- произвольный полином, то общее решение будет:

$$b_{p1} = A_pf_{p1} + qb_{p0},$$

$$a_{p1} = B_pf_{p1} - qa_{p0}$$

.

Вопрос: чем плохо частное решение и почему мы хотим иметь общее?
$QUESTION$
$out:$

$QUESTION$

Каждое произведение $A_p f_{p1}$ и $B_p f_{p1}$ может иметь степень больше, чем f_{p1} на степень полинома A_p или B_p, соответственно. Конечно, в сумме (2) они взаимно уничтожатся. Поэтому надо сразу найти такое частное решение, которое будет иметь наименьшую степень.

Возьмем в качестве q – целую часть частного от деления $B_p f_{p1}$ на a_{p0}, т.е. $\mathbf{quotient}(B_p f_{p1}, a_{p0})$.

Тогда полином $B_p f_{p1} - q a_{p0}$ будет равен остатку при этом делении и его степень будет меньше, чем a_{p0}.

Понятно, что это наименьшая возможная степень у полинома $B_p f_{p1} - q a_{p0}$.

Мы получим в кольце $Z/pZ[x]$:

$a_{p1} = \mathbf{remainder}(B_p\ f_{p1}, a_{p0});$

$b_{p1} = A_p\ f_{p1}\ +\ b_{p0}\mathbf{quotient}(B_p\ f_{p1}, a_{p0});$

$\mathbf{print}(a_{p1}, b_{p1});$

$out:$

$a_{p1} = 2x^2 + 1$

$b_{p1} = -8x + 1$

А может ли быть у b_1 высокая степень?

Как видно из равенства (2) сумма степеней b_1 и a_0 не может быть больше степени f_1.

Мы нашли $A_1 = a_0 + pa_1$, $B_1 = b_0 + pb_1$.

$SPACE = Z[x]; a_1 = \mathbf{toNewRing}(a_{p1}); b_1 = \mathbf{toNewRing}(b_{p1});$

$A_1 = a_0 + pa_1; B_1 = b_0 + pb_1;$

Это второй этаж. Проверим это;

$F_1 = f - A_1 B_1; p2 = p^2; R_1 = \mathbf{mod}(F_1, p2); \mathbf{print}(A_1, B_1, R_1);$

$out:$

$A_1 = x^3 + 25x^2 + 13$

$B_1 = x^3 - 83x + 14$

$R_1 = 0$

Как подняться выше?

(2) Пусть $p^2 a_2$ и $p^2 b_2$ искомые добавки к A_1 и B_1, такие, что

$$F_2 = (A_1 + p^2 a_2)(B_1 + p^2 b_2) = \mathbf{mod}(f, p^3). \qquad (3)$$

Так как $F_2 = A_1 B_1 + p^2 f_2$ то

$$f_2 = A_1\ b_2 + B_1\ a_2 = (f - A_1 B_1)/p^2\ ; \mathbf{print}(f_2);$$

Достаточно знать a_2 и b_2 в $Z/pZ[x]$,так как равенство (3) не изменится при добавлении к ним любого кратного p. Вспомним, что $A_1 = a_0 + pa_1$, $B_1 = b_0 + pb_1$ и

будем решать уравнение

$$a_0 b_2 + b_0 a_2 = f_2. \qquad (4)$$

в кольце $Z/pZ[x]$. Можно воспользоваться алгоритмом, который применяли на первом шаге:

$out:$

$f_2 = x^4 + 25x^3 + 13x$

$SPACE = Zp32[x]; MOD32 = 11; f_{p2} = \mathbf{toNewRing}(f_2);$

$a_{p2} = \mathbf{remainder}(B_p\ f_{p2}, a_{p0});$
$b_{p2} = A_p\ f_{p2}\ +\ b_{p0}\mathbf{quotient}(B_p\ f_{p2}, a_{p0});$
$\mathbf{print}(a_{p2}, b_{p2});$
Отметим, что здесь те же A и B, что и на предыдущем шаге.-

$out:$

$a_{p2} = 0$
$b_{p2} = x$

$SPACE = Z[x]; a_2 = \mathbf{toNewRing}(a_{p2}); b_2 = \mathbf{toNewRing}(b_{p2});$
$A_2 = (A_1 + p^2 a_2); B_2 = (B_1 + p^2 b_2);$
$F_3 = f - A_2 B_2; \mathbf{print}(F_3, A_2, B_2);$
$out:$

$F_3 = 0$
$A_2 = x^3 + 25x^2 + 13$
$B_2 = x^3 + 38x + 14$

Когда заканчивается подъем?

Когда разность $f - A_k B_k$ на очередном шаге будет равна нулю.

А если исходный полином в целых числах не раскладывается на множители, то надо поднимать до такой степени n при которой число p^n будет больше, чем $2\alpha + 1$, где α - наибольший возможный коэффициент.

Если ноль в разности не был получен до этого, то дальше подниматься нет смысла.

Такой метод решения известен под названием «Линейный подьем по Гензелю ».

[Курт Вильгельм Себастьян Гензель (Kurt Wilhelm Sebastian Hensel, 1861—1941) родился в Кёнигсберге. Учился в Берлинском и Боннском университетах у Леопольда Кронекер и Карла Вейерштрасса. Преподавал в Марбургский университет (полный профессор с 1901). В 1897 году Гензель открыл p-адические числа.]

(Известен еще и квадратичный подъем, когда степени берутся не порядке $p^1, p^2, p^3, ...$, а порядке $p^1, p^2, p^4, p^8....$ Для этого (0) нужно было бы расписать по таким степеням, а в формуле (3) брать модуль не по p^3, а сразу по p^4, а потом P^8 и так далее. Но тогда требуется пересчитывать расширенный алгоритм Евклида на каждом шаге. Такой алгоритм, в итоге, имеет большую сложность, чем линейный.)

END
$out:$

END
