02. Факторизация полинома, когда старший коэффициент не равен одному.

$SPACE = Z[x];$
Требуется в кольце $Z[x]$ разложить на множители полином
$f = 6x^6 + 109x^5 + 472x^4 + 1033x^3 + 1031x^2 + 668x + 272$
у которого старший коэффциент
$lc = \textbf{leadingCoeff}(f);$
не равен одному. Если известно, что образ этого полинома
$F_0 = 6x^6 + 5x^5 + 4x^4 + 6x^3 + 4x^2 + 5x - 1;$
при отображении $Z - - > Z_p$
$p = 13;$
раскладывается на взаимно простые множители
(они нормированы в Z_p так, чтобы старший коэффициент был равен 1):
$a_0 = x^3 - 6x^2 - 7x - 5; b_0 = x^3 - 4x^2 + x - 3;$
$\textbf{print}(a_0, b_0, lc);$
$out:$

$a_0 = x^3 - 6x^2 - 7x - 5$
$b_0 = x^3 - 4x^2 + x - 3$
$lc = 6$

Отступление **1**, поясняющее, как были получены входные данные задачи.
Были выбраны случайные полиномы, которые будут вычислены в конце параграфа:
$a0 = 2x^3 + 27x^2 + 12x + 16; \quad b0 = 3x^3 + 14x^2 + 29x + 17;$
Найдено их произведение, которое стало входным полиномом
$f = a0 \cdot\ b0;$
$out:$

$6x^6 + 109x^5 + 472x^4 + 1033x^3 + 1031x^2 + 668x + 272$

Отступление **2**. Для вычисления образов в Z_p, задано простое поле и в него отображены сомножители:
$SPACE = Zp32[x]; MOD32 = 13; f_{p0} = \textbf{toNewRing}(f);$
$a_{p0} = \textbf{toNewRing}(a0); b_{p0} = \textbf{toNewRing}(b0);$
Для нормировки полиномов надо разделить каждый из них на старший коэффициент:
$lca = \textbf{leadingCoeff}(a_{p0}); lcb = \textbf{leadingCoeff}(b_{p0});$
$a_{p0} = a_{p0}/lca; b_{p0} = b_{p0}/lcb;$
$c_{0p} = a_{p0} b_{p0};$
Проверим, что ошибок нет, и следующая разность равна нулю:
$sub = lca \cdot\ lcb\ a_{p0} b_{p0} - f_{p0};$
$\textbf{print}(a_{p0}, b_{p0}, f_{p0}, sub);$
$out:$

$a_{p0} = x^3 - 6x^2 - 7x - 5$
$b_{p0} = x^3 - 4x^2 + x - 3$
$f_{p0} = 6x^6 + 5x^5 + 4x^4 + 6x^3 + 4x^2 + 5x - 1$
$sub = 0$

Проверка входных данных перед началом решения задачи.

Убедимся, что входные данные верные. Найдем образы в конечном поле:

$SPACE = Zp32[x]; MOD32 = 13;$
$a_{p0} = \mathbf{toNewRing}(a_0); b_{p0} = \mathbf{toNewRing}(b_0);$
$f_{p0} = \mathbf{toNewRing}(f); c_{p0} = a_{p0} b_{p0};$
Разделим полиномы и убедимся, что частное – это число, а в остатке будет ноль:
$remainder = \mathbf{remainder}(f_{p0}, c_{p0}); quotient = \mathbf{quotient}(f_{p0}, c_{p0});$
$\mathbf{print}(f_{p0}, c_{p0}, remainder, quotient)$
$out:$

$f_{p0} = 6x^6 + 5x^5 + 4x^4 + 6x^3 + 4x^2 + 5x - 1$
$c_{p0} = x^6 - 10x^5 + 5x^4 + x^3 + 5x^2 + 3x + 2$
$remainder = 0$
$quotient = 6$

Р Е Ш Е Н И Е

Дополнительная проблема заключается в том, что «настоящие» сомножители, даже в простом поле, остаются неизвестными, так как не понятно какой из полиномов-сомножителей и на какой делитель старщего члена надо домножать.

Один из простых путей решения этой проблемы состоит в том, чтобы задачу сделать симметричной по двум сомножителям. Домножим исходный полином на его старший коэффициент
$l_{pc} = \mathbf{leadingCoeff}(f_{p0});$
$f_{p0} = l_{pc} f_{p0};$
$a_{p0} = l_{pc} a_{p0};$
$b_{p0} = l_{pc} b_{p0};$
Будем рассматривать задачу «подъема» таких сомножителей с одинаковыми старшими коэффициентами:
$\mathbf{print}(f_{p0},\ a_{p0}, b_{p0})$
$out:$

$f_{p0} = 10x^6 + 4x^5 + 11x^4 + 10x^3 + 11x^2 + 4x + 7$
$a_{p0} = 6x^3 - 10x^2 - 3x - 4$
$b_{p0} = 6x^3 - 11x^2 + 6x - 5$

Теперь можно вернуться к прежнему алгоритму. Домножим полином f на его старший коэффициент. Найдем
$SPACE = Z[x]; F = \mathbf{leadingCoeff}(f) \cdot f;$
$a_0 = \mathbf{toNewRing}(a_{p0}); b_0 = \mathbf{toNewRing}(b_{p0});$
$f_1 = (F - a_0 b_0)/p;$
$\mathbf{print}(a_0, b_0, f_1)$
Тут должно произойти сокращение на p
$out:$

$a_0 = 6x^3 - 10x^2 - 3x - 4$
$b_0 = 6x^3 - 11x^2 + 6x - 5$
$f_1 = 60x^5 + 208x^4 + 483x^3 + 470x^2 + 309x + 124$

Один шаг вверх по стереням p сводится к нахождению неизвестных сомножителей b_1 и a_1 в Евклидовом кольце $Z_p[x]$ в равенстве

$$a_0 b_1 + b_0 a_1 = f_1.$$

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

$$Aa_0 + Bb_0 = 1.$$

Найдем их
$SPACE = Zp32[x]; f_{p1} = \mathbf{toNewRing}(f_1);$
$VP = \mathbf{extendedGCD}(a_{p0}, b_{p0}); VP = (vp_i); A_p = vp_2; B_p = vp_3; a_{p1} = B_p f_{p1}; b_{p1} = A_p f_{p1};$
И проверим, что следующее тождественное равенство нулю выполняется:
$Sub = a_{p0} A_p f_{p1} + b_{p0} B_p f_{p1} - \ f_{p1};$
$\mathbf{print}(VP, Sub);$
$out:$

$VP = [1, x^2 + 6x - 2, -x^2 - 4x + 4]$
$Sub = 0$

$SPACE = Zp32[x];$
$b_{p1} = A_p \ f_{p1} \ + \ b_{p0}\mathbf{quotient}(a_{p1}, a_{p0});$
$a_{p1} = \mathbf{remainder}(a_{p1}, a_{p0});$
$\mathbf{print}(a_{p1}, b_{p1});$
$out:$

$a_{p1} = -6x^2 + 3x - 9$
$b_{p1} = 3x^2 - 9x + 3$

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. Полином F_2 должен сократиться на p^2 ;
$F_2 = F - A_1 B_1; f_2 = F_2/p^2;$ $\mathbf{print}(A_1, B_1, f_2);$
$out:$

$A_1 = 6x^3 - 88x^2 + 36x - 121$
$B_1 = 6x^3 + 28x^2 - 111x + 34$
$f_2 = 6x^5 + 34x^4 - 24x^3 + 98x^2 - 63x + 34$

$SPACE = Zp32[x]; \quad f_{p2} = \mathbf{toNewRing}(f_2);$
$a_{p2} = \mathbf{remainder}(B_p \ f_{p2}, a_{p0});$
$b_{p2} = A_p \ f_{p2} \ + \ b_{p0}\mathbf{quotient}(B_p \ f_{p2}, a_{p0});$
$\mathbf{print}(f_{p2}, a_{p2}, b_{p2});$
$out:$

$f_{p2} = 6x^5 + 8x^4 - 11x^3 + 7x^2 - 11x + 8$
$a_{p2} = x^2 + 1$
$b_{p2} = x$

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

$F_3 = 0$
$A_2 = 6x^3 + 81x^2 + 36x + 48$
$B_2 = 6x^3 + 28x^2 + 58x + 34$

Но мы решили задачу, в которой исходный полином был домножен на первый коэффициент.

Чтобы вернуться к разложению исходного полинома нужно последовательно сокращать найденные полиномы на делители

первого коэффициента:

$B_3 = \mathbf{cancel}(B_2/lc); A_3 = \mathbf{cancel}(A_2/lc); [B_3, A_3]$

$out:$

$[((3x^3 + 14x^2 + 29x + 17)/3), ((2x^3 + 27x^2 + 12x + 16)/2)]$

Выделим у этих дробей числители и знаменатели:

$Aout = \mathbf{num}(A_3); Bout = \mathbf{num}(B_3); da = \mathbf{denom}(A_3); db = \mathbf{denom}(B_3);$

Следовательно, искомые сомножители это $Aout$ и $Bout$. Свободный числовой множитель:

$Nout = lc/(da \cdot db);$

Проверим полученное решение:

$Sub = f - Nout \cdot Aout \cdot \ Bout;$

$\mathbf{print}(Bout, Aout, \quad Nout, Sub);$

$out:$

$Bout = 3x^3 + 14x^2 + 29x + 17$

$Aout = 2x^3 + 27x^2 + 12x + 16$

$Nout = 1$

$Sub = 0$
