Пример Кнута для $\mathbf{Z}[\mathbf{x}]$

$SPACE = Z[x];$

Дональд Кнут во 2-м томе 'Искусство программирования' рассматривает пример факторизации полинома

$f = x^8 + x^6 + 10x^4 + 10x^3 + 8x^2 + 2x + 8.$

Так как уже понятно из чего складывается алгоритм факторизации, то рассмотрив его в полном виде на этом примере.

Для начала найдем

$\mathbf{GCD}(f, D_x(f))$

$out:$

1

Так как GCD=1, то кратных сомножителей у полинома нет.

Обозначим:

$p = 13$ – характеристику поля

$deg = \mathbf{degree}(f); degPlus1 = deg + 1;\ one = 1;$

$N = p \cdot (deg - 1); W = \mathbf{O}_N; W = (w_i);$

Образуем последовательность чисел, кратных р:

$K = \mathbf{O}_{deg}; K = (k_i);$

$for(j = 1; j \leq deg; j = j + 1)\{k_j = (j - 1) \cdot p;\}\mathbf{print}(K);$

$out:$

$K = [0, 13, 26, 39, 52, 65, 78, 91]$

Возьмем конечное поле Z_{13}, отобразим в него полином и проверим не появились ли кратные множители в этом поле. Если появятся, то надо будет поменять поле.

$SPACE = Zp32[x]; MOD32 = 13; f_p = \mathbf{toNewRing}(f);$

$GCD_p = \mathbf{GCD}(f_p, D_x(f_p));$

$out:$

1

Выбор конечного поля оказался удачным. Будем исать сомножители в этом поле.

Вычислим образы w_j для мономов x^j в кольцо Z_{p,f_p}.

С начала для тех мономов, у которых степень меньше, чем deg:

$temp = x;$

$for(i = one; i < deg\ ; i = i + one)\{temp = temp \cdot x; w_i = temp;\};$

$D = x^{deg} - f_p; w_{deg} = D; T = D;$

Теперь для тех мономов, у которых степень больше, чем deg:

$for(i = degPlus1; i \leq N; i = i + 1)\{$

$\quad if(\mathbf{degree}(T) == deg - 1)\{lc = \mathbf{leadingCoeff}(T);\}else\{\ lc = 0;\}$

$\quad T = lc \cdot D + x \cdot T - lc \cdot\ x^{deg};\ w_i = T;\}$

Составляем матрицу:

$V = \mathbf{O}_{deg}; V = (v_i); v_1 = \mathbf{O}_{deg}; VF = v_1; VF = (vF_i); vF_{deg} = 1;$

$for(j = 2; j \leq deg; j = j + 1)\{u = k_j; v_j = \mathbf{toVectorDence}(w_u, deg);\}\quad V$

$out:$

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 11 & 5 & -1 & 10 & 11 & 7 & 1 & 2 \\ -11 & -6 & 4 & 0 & -10 & -9 & -7 & -10 \\ 3 & 2 & 6 & 1 & -8 & -7 & -10 & -9 \\ -2 & 3 & 1 & 3 & 8 & -5 & 11 & 2 \\ -4 & -3 & 7 & 2 & -7 & 8 & 11 & 6 \\ -1 & -6 & -2 & 0 & -3 & -6 & -2 & -8 \\ -1 & -4 & -2 & 0 & 5 & -1 & 3 & 3 \end{pmatrix}$$

Повернем матрицу по часовой стрелке, первая строка станет последним столбцом:
$Q_p = \mathbf{O}_{deg,deg}; Q_p = (elQ_{i,j});$
$for(j = one; j \leq deg; j = j + one)\{$
$U = v_{deg+one-j}; U = (u_i);$
$for(i = one; i \leq deg; i = i + one)\{elQ_{i,j} = u_i;\}\}\ Q_p$
$out:$

$$\begin{pmatrix} -1 & -1 & -4 & -2 & 3 & -11 & 11 & 0 \\ -4 & -6 & -3 & 3 & 2 & -6 & 5 & 0 \\ -2 & -2 & 7 & 1 & 6 & 4 & -1 & 0 \\ 0 & 0 & 2 & 3 & 1 & 0 & 10 & 0 \\ 5 & -3 & -7 & 8 & -8 & -10 & 11 & 0 \\ -1 & -6 & 8 & -5 & -7 & -9 & 7 & 0 \\ 3 & -2 & 11 & 11 & -10 & -7 & 1 & 0 \\ 3 & -8 & 6 & 2 & -9 & -10 & 2 & 1 \end{pmatrix}$$

Найдем ядро оператора и транспонируем его:
$B = Q_p - \mathbf{I}_{deg,deg};$
$ker = \mathbf{kernel}(B); Ker = ker^T;$

Проверим дает ли произведение B*ker нулевую матрицу:
$Check = B \cdot ker; ZeroCheck = Check^T;\ m = \mathbf{rowNumb}(Ker); \mathbf{print}(Ker, ZeroCheck, m);$
$out:$

$$Ker = \begin{pmatrix} 7 & 3 & 8 & 6 & 11 & 1 & 0 & 0 \\ -7 & -8 & -7 & 1 & -11 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$ZeroCheck = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$m = 3$

Каждому базисному вектору ядра ker, соответствует один полином - решение. Последнему вектору соответствует решение, которое является константой, поэтому мы его не берем.

$P = \mathbf{O}_{deg}; P = (pol_i);$ Это массив для хранения полученных полиномов.
$FP = \mathbf{O}_{deg}; FP = (fp_i);$ Это массив искомых полиномов-сомножителей.
$for(i = one; i \leq m; i = i + 1)\{pol_i = \mathbf{vectorToPolynom}(\mathbf{takeRow}(Ker, i));\}P$
$out:$

$[7x^7 + 3x^6 + 8x^5 + 6x^4 + 11x^3 + x^2, -7x^7 - 8x^6 - 7x^5 + x^4 - 11x^3 + x, 1, 0, 0, 0, 0, 0]$

Ищем НОД полинома f_p с этими полиномами, с добавленными свободными членами.

Подсчитываем количество найденных сомножителей и записываем их в массив FP, пока их число не станет равно m

$factNumb = 0; j = 1; i = 1;$
$while(m > factNumb)\&(m > j)\{$
$temp = pol_j + i; gcd = \mathbf{GCD}(temp, f_p); i = i + 1; if(i == 0)\{j = j + 1;\}$
$if(\neg(\mathbf{isOne}(gcd)))\{factNumb = factNumb + one; fp_{factNumb} = gcd;\}$
$\}$
$\mathbf{print}(factNumb, FP, m);$
$out:$

$factNumb = 3$
$FP = [x^3 - 5x^2 + 4x - 1, x + 3, x^4 + 2x^3 + 3x^2 + 4x + 6, 0, 0, 0, 0, 0]$
$m = 3$

Сделаем проверку найденных полиномов:
$Prod = fp_1; i = 2;\ while(factNumb > i - 1)\{Prod = Prod \cdot\ fp_i; i = i + 1;\}$
$sub = f_p - Prod; \mathbf{print}(i, sub);$
$out:$

$i = 4$
$sub = 0$

Проверим, что тут нет готовых сомножителей полинома f в кольце Z. Для этого разделим и найдем остатки от деления.

$SPACE = Z[x]; M = \mathbf{toNewRing}(m); FP_z = \mathbf{O}_M; FP = (fpz_i);$
$for(i = 1; i \leq M; i = i + 1)\{fpz_i = \mathbf{toNewRing}(fp_i); g = \mathbf{remainder}(f, fpz_i); \mathbf{print}(g);\}$

Сформируем два сомножителя и недостающую часть произведения следующим образом:
$a_0 = fpz_1 \cdot fpz_2; b_0 = fpz_3;$
$f_1 = (f - a_0 b_0)/p; \mathbf{print}(f_1);$

Заметим, что существует $\binom{3}{2} = 3$ разных наборов, которые нужно пересмотреть, чтобы утверждать,

что полином не разложим в Z.

$out:$

$g = 6461x^2 - 5928x + 1586$
$g = 7904$
$g = -26x^2 - 26x - 52$
$f_1 = x^6 + x^5 + 2x^4 + 3x^3 + 3x^2 - 4x + 2$

Подъем сомножителей в кольце **Z**

Найдем границу для подъема коэффициентов у делителя g степени m полинома f, исходя из неравенства:

$$||g|| < 2^m ||f||,$$

где $||f||$ обозначает корень квадратный из суммы квадратов всех коэффициентов полинома f.

Так как полином f имеет степень deg, то в случае факторизации, хоть один сомножитель имеет степень $m \leq \mathbf{floor}(deg/2)$. Вычислим логарифм по основанию p, чтобы получить максимальное число шагов подъема.

$SPACE = R64[x]; V = \mathbf{toVectorDence}(f); V = (v_i); nn = \mathbf{size}(V); sum = v_{nn} \cdot v_{nn};$
$for(i = 1; nn > i; i = i + 1)\{sum = sum + v_i \cdot v_i;\}$
$valF = \sqrt{(}sum);$
$valG = 2^{\mathbf{floor}(deg/2)} valF;$
$stepsNumber = \mathbf{value}(\mathbf{log}_p(valG));$
$\mathbf{print}(valF, valG, stepsNumber);$

$out:$

$valF = 18.28$
$valG = 292.41$
$stepsNumber = 2.21$

Так как $2 < 2.21 < 3$, следовательно, достаточно найти разложение по модулю $\mathbf{p^3}$.

Если за три шага не удается получить разложение полинома f над Z, следовательно такого разложения нет.

Один шаг вверх $p - - > p^2$ сводится к нахождению неизвестных сомножителей b_1 и a_1 в Евклидовом кольце $Z_p[x]$ в равенстве

$$a_{p0}b_{p1} + b_{p0}a_{p1} = f_{p1}.$$

$SPACE = Zp32[x];\ a_{p0} = \mathbf{toNewRing}(a_0);\ b_{p0} = \mathbf{toNewRing}(b_0); f_{p1} = \mathbf{toNewRing}(f_1);$
$VP = \mathbf{extendedGCD}(a_{p0}, b_{p0});$
$VP = (vp_i); A_p = vp_2; B_p = vp_3; a_{p1} = B_p f_{p1}; b_{p1} = A_p f_{p1};$
И проверим, что выполняется следующее равенство нулю:
$Sub = a_{p0}b_{p1} + b_{p0}a_{p1} - \ f_{p1};$
$b_{p1} = A_p f_{p1} + \ b_{p0}\mathbf{quotient}(B_p f_{p1}, a_{p0});$
$a_{p1} = \mathbf{remainder}(B_p f_{p1}, a_{p0});$
$\mathbf{print}(a_{p1}, b_{p1}, VP, Sub);$
$out:$

$a_{p1} = -x^3 - x^2 + 11x + 6$
$b_{p1} = x^3 + 6x^2 - 8x - 6$
$VP = [1, 6x^3 + 3, -6x^3 - 2x^2 - 3x + 6]$
$Sub = 0$

Мы нашли $A_1 = a_0 + pa_1$ и $B_1 = b_0 + pb_1$ по модулю p^2. Проверим правильность.

$SPACE = Z[x]; a_1 = \mathbf{toNewRing}(a_{p1}); b_1 = \mathbf{toNewRing}(b_{p1});$
$A_1 = a_0 + pa_1; B_1 = b_0 + pb_1;$
Полином f_2 должен сократиться на p^2 ;
$f_2 = f - A_1B_1; f_2 = f_2/p^2;\ \mathbf{print}(A_1, B_1, f_2);$
$out:$

$A_1 = x^4 - 15x^3 - 24x^2 + 154x + 75$
$B_1 = x^4 + 15x^3 + 81x^2 - 100x - 72$
$f_2 = x^6 + 9x^5 - 11x^4 - 101x^3 + 45x^2 + 110x + 32$

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

$f_{p2} = x^6 + 9x^5 - 11x^4 - 10x^3 + 6x^2 + 6x + 6$
$a_{p2} = 2x^3 + 10x^2 - x - 1$
$b_{p2} = 11x^3 + 9x^2 + 6x + 9$

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

$f_3 = f - A_2B_2; f_3 = f_3/p^3;$ **print**(f_3, A_2, B_2); f_3 должен сократитьсяна p^3.
$out:$

$f_3 = -x^7 - 277x^6 - 1657x^5 - 1338x^4 - 2689x^3 - 2626x^2 - 865x - 1387$
$A_2 = x^4 + 323x^3 + 1666x^2 - 15x + 2103$
$B_2 = x^4 + 1874x^3 + 1602x^2 + 914x + 1449$

То, что полином f_3 сократился на p^3, говорит о том, что было правильно найдено разложение по модулю p^3.

Однако, разложение исходного полинома f не найдено. Теперь возьмем другое сочетание сомножителей:
$a_0 = fpz_1 \cdot fpz_3; b_0 = fpz_2;$ **print**(a_0, b_0);
$out:$

$a_0 = x^7 - 3x^6 - 3x^5 - 4x^4 - 4x^3 - 17x^2 + 20x - 6$
$b_0 = x + 3$

Подъем второго варианта сомножителей в кольцо **Z**

$SPACE = Zp32[x];$ $a_{p0} =$ **toNewRing**(a_0); $b_{p0} =$ **toNewRing**(b_0); $f_{p1} =$ **toNewRing**(f_1);
$VP =$ **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 выполняется следующее равенство нулю :
$Sub = a_{p0}b_{p1} + b_{p0}a_{p1} - f_{p1};$
print(VP, Sub);
$b_{p1} = A_p f_{p1} + b_{p0}$**quotient**$(B_p f_{p1}, a_{p0})$;
$a_{p1} =$ **remainder**$(B_p f_{p1}, a_{p0})$;
print(a_{p1}, b_{p1})
$out:$

$VP = [1, -6, 6x^6 + 3x^5 - x^4 + 5x^3 + 2x - 3]$
$Sub = 0$
$a_{p1} = 8x^6 + 5x^5 + x^4 + 6x^3 + 5x^2 - 5x + 2$
$b_{p1} = -8$

Мы нашли $A_1 = a_0 + pa_1$ и $B_1 = b_0 + pb_1$ по модулю p^2. Проверим правильность.

$SPACE = Z[x]; a_1 =$ **toNewRing**(a_{p1}); $b_1 =$ **toNewRing**(b_{p1});
$A_1 = a_0 + pa_1; B_1 = b_0 + pb_1;$
Полином f_2 должен сократиться на p^2 ;
$f_2 = f - A_1B_1; f_2 = f_2/p^2;$ **print**(A_1, B_1, f_2);
$out:$

$A_1 = x^7 + 101x^6 + 62x^5 + 9x^4 + 74x^3 + 48x^2 - 45x + 20$
$B_1 = x - 101$
$f_2 = 60x^6 + 37x^5 + 5x^4 + 44x^3 + 29x^2 - 27x + 12$

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

$f_{p2} = 8x^6 + 11x^5 + 5x^4 + 5x^3 + 3x^2 - x - 1$
$a_{p2} = 8x^5 + 5x^3 + 3x^2 - 6x - 9$
$b_{p2} = 0$

$SPACE = Z[x]; a_2 = \mathbf{toNewRing}(a_{p2}); b_2 = \mathbf{toNewRing}(b_{p2});$
$A_2 = (A_1 + p^2 a_2); B_2 = (B_1 + p^2 b_2);$
$f_3 = f - A_2 B_2; f_3 = f_3/p^3; \mathbf{print}(f_3, A_2, B_2);$

То, что полином f_3 сократился на p^3, говорит о том, что было правильно найдено разложение по модулю p^3.

Однако, разложение исходного полинома f не найдено. Теперь возьмем другое сочетание сомножителей:

$a_0 = fpz_2 \cdot fpz_3; b_0 = fpz_1; \mathbf{print}(a_0, b_0);$
$out:$

$f_3 = 81x^6 - 139x^5 - 102x^4 - 74x^3 + 174x^2 + 6x - 236$
$A_2 = x^5 - 424x^4 + 1270x^3 - 507x^2 - 788x + 850$
$B_2 = x^3 + 424x^2 + 550x + 610$
$a_0 = x^5 + 5x^4 + 9x^3 + 13x^2 + 18x + 18$
$b_0 = x^3 - 5x^2 + 4x - 1$

Подъем третьего варианта сомножителей в кольцо $\mathbf{Z}$

$SPACE = Zp32[x];\ a_{p0} = \mathbf{toNewRing}(a_0);\ b_{p0} = \mathbf{toNewRing}(b_0); f_{p1} = \mathbf{toNewRing}(f_1);$
$VP = \mathbf{extendedGCD}(a_{p0}, b_{p0});$
$VP = (vp_i); A_p = vp_2; B_p = vp_3; a_{p1} = B_p f_{p1}; b_{p1} = A_p f_{p1};$
И проверим, что следующее равенство нулю выполняется:
$Sub = a_{p0} b_{p1} + b_{p0} a_{p1} - f_{p1};$
$\mathbf{print}(VP, Sub);$
$out:$

$VP = [1, -6x, 6x^3 - 5x^2 + 5x - 1]$
$Sub = 0$

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

$a_{p1} = 6x^4 + 6x^3 - x^2 + 3x - 1$
$b_{p1} = 7x^2 - 10x + 8$

Мы нашли $A_1 = a_0 + pa_1$ и $B_1 = b_0 + pb_1$ по модулю p^2. Проверим правильность.

$SPACE = Z[x]; a_1 = \mathbf{toNewRing}(a_{p1}); b_1 = \mathbf{toNewRing}(b_{p1});$
$A_1 = a_0 + pa_1; B_1 = b_0 + pb_1;$
Полином f_2 должен сократиться на p^2 ;
$f_2 = f - A_1 B_1; f_2 = f_2/p^2;\ \mathbf{print}(A_1, B_1, f_2);$
$out:$

$A_1 = x^5 + 83x^4 + 87x^3 + 57x + 5$
$B_1 = x^3 + 86x^2 - 126x + 103$

$f_2 = -x^7 - 42x^6 + 17x^5 + 14x^4 - 82x^3 + 40x^2 - 31x - 3$

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

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

$SPACE = Z[x]; a_2 = \mathbf{toNewRing}(a_{p2}); b_2 = \mathbf{toNewRing}(b_{p2});$
$A_2 = (A_1 + p^2 a_2); B_2 = (B_1 + p^2 b_2);$
$f_3 = f - A_2 B_2; f_3 = f_3/p^3; \mathbf{print}(f_3, A_2, B_2);$
$out:$

$f_3 = 81x^6 - 139x^5 - 102x^4 - 74x^3 + 174x^2 + 6x - 236$
$A_2 = x^5 - 424x^4 + 1270x^3 - 507x^2 - 788x + 850$
$B_2 = x^3 + 424x^2 + 550x + 610$

ЗАКЛЮЧЕНИЕ: Заданный полином f не раскладывается на сомножители с целыми коэффициентами.
END
$out:$

END
