1. Znajdź rozkład na czynniki wielomianu $P = x^5+5x^4+6x^3+4x^2+3x+9$ modulo 11, obliczając $GCD(x^{11^m} - x, P)$ dla różnych m. Użyj komputera do oblicznia GCD i potęg.

2. Znajdź rozkład na czynniki wielomianu $P = x^6 + x^5 + 4x^4 + 7x^3 + x^2 + 8x + 2$ modulo 11, obliczając $GCD(Q^l - 1, P)$ (i dwie pozostałe możliwości) dla odpowiedniego l i różnych Q. Użyj komputera do oblicznia GCD i potęg.

Wskazówka: P jest produktem dwu czynników nieprzywiedlnych stopnia 3.

3. Niech $P = x^5 + 23x^4 + 14x^3 + 442x^2 + 20x - 25$. Oblicz rozkład P na czynniki rozkładając P na czynniki modulo 7 i następnie stosując podnoszenie Hensla do odtworzenia czynników nad liczbami całkowitymi. Uwaga: w kroku podnoszenia można użyć trójargumentowe `extendedEuclidean`.

4. Niech $P = 6x^4+63x^3+51x^2+630x-90$. Oblicz rozkład P na czynniki rozkładając P na czynniki modulo 17 i następnie stosując podnoszenie Hensla do odtworzenia czynników nad liczbami całkowitymi. Przy tym najpierw znajdź czynniki $6P$ z najwyższym współczynnikiem 6.

5. Oblicz największy wspólny dzielnik R wielomianów $P(x) = x^3 + 190x^2 + 504x + 59535$ i $Q(x) = x^4 + 4x^3 + 763x^2 + 1390x + 140175$ następującą metodą: najpierw obliczycz największy wspólny dzielnik modulo 37, co daje równości $P(x) = P_1(x)R(x) \mod 37$ i $Q(x) = Q_1(x)R(x) \mod 37$. Następnie zastosuj podnoszenie Hensla do otrzymanego rozkładu i dostań odpowiedni rozkład Q modulo 37^2.

6. Potegi x^{p^k} można obliczać bazując na wzorze $x^{p^{k+l}} = (x^{p^k})^{p^l}$. Zapoznaj się z przykładowym programem `modkomp.input`. Funkcja `modcompose` oblicza $pol1 \circ pol2$ modulo $modp$. Użyj tą funkcję do obliczenia $x^{p^k} \mod Q$ dla $p = 31$, $k = 1, \ldots, 5$, $Q = x^{10} + 7x^9 + x^2 + 1$.

7. Niech

$$A = \begin{pmatrix} 5 & 16 \\ 4 & 12 \end{pmatrix}$$

Rozwiąż układ równań $Ax = y$ gdzie $y = (6, -1)$ obliczając metodą podnoszenia Hensla rozwiązanie modulo 5^3. Do poszczególnych kroków obliczeń użyj komputera.

8. Porównaj koszt rozwiązywnia układu równań o współczynnikach cał-

kowitych metodą bazowaną na chińskim twierdzeniu o resztach i metodą podnoszenia Hensla. W szczególności jak wpływa wielkość elementów macierzy A zadającej układ równań na koszt rozwiązania.

9. Uzasadnij podane na wykładzie lematy o jednoznaczności rekonstrukcji wymiernej.

10. Wiadomo że $a/b = 838373812589632458095913892045735861 05$ modulo $92795652982522074438278995413938676481$, $|a| < 10^{17}$, $0 < b < 10^{17}$. Znajdź a i b (można użyć przykładową procedurę rekonstrukcji liczb wymiernych).

11. Przerób przykładową procedurę rekonstrukcji wymiernej tak by pracowała dla wielomianów nad ciałem skończonym. Użyj jej do wyznaczenia wielomianów a i b o współczynnikach w ciele 37-elementowym takich że $a/b = 19x^8 + 23x^7 + 36x^6 + 6x^5 + 7x^4 + 17x^3 + 18x^2 + 25x + 9$, $\deg(a) = 3$, $\deg(b) = 4$.

12. Przerób przykładową procedurę podnoszenia Hensla tak by odtwarzała rozkład wielomianu dwu zmiennych nad ciałem skończonym mając dany rozkład wielomianu jednej zmiennej otrzymanego przez podstawienie zadanej wartości za jedną ze zmiennych.

13. Rugownik wielomianów dwu zmiennych nad ciałem (gdzie jedna jest zmienną główną a druga parametrem traktowanym jako element pierścienia współczynników) moża obliczać podstawiając pod parametr różne wartości, obliczając rugownik i odtwarzając wynik poprzez interpolację. Oszacuj ile wartości parametru jest potrzebne w zależności od stopni wielomianów wejściowych. Zaprogramuj funkcję obliczającą rugownik tą metodą, traktując funkcję obliczającą rugownik wielomianów nad ciałem za daną (można użyć wbudowaną funkcję `resultant` albo funkcję z zadania 1).

14. Przy podnoszeniu Hensla mając dany rozkład wielomianu modulo p^k można otrzymać rozkład modulo p^{2k}. Wyprowadź i uzasadnij odpowiednie wzory. Porównaj koszt takiego podejścia z przedstawionym na wykładzie przejściem od p^k do p^{k+1}.

15. Popularną metodą generownia liczb pseudolosowych jest użycie rejestrów przesuwających z liniowym sprzężeniem zwrotnym (ang. LFSR). Kod w C może wyglądać nastepująco:

```
uint16_t stan = 1;
const uint16_t pol = 1<<k | 1<<l | 1<<m | 1;
```

```
uint16_t get_random(void)
{
    stan = (stan&(1u<<15u))?((stan<<1)^pol):(stan<<1);
    return stan;
}
```

gdzie k, l, m są stałymi. Niech wielomian $p = x^{16} + x^k + x^l + x^m + 1$. Uzasadnij że jeśli p jest nierozkładalny i x jest elementem maksymalnego rzędu w $GF(2^{16})$ (taki wielomian nazywamy prymitywnym) to zmienna `stan` przebiega przez wszystkie niezerowe ciągi szesnastobitowe. Odwrotenie, jeśli `stan` przebiega przez wszystkie niezerowe ciągi szesnastobitowe to wielomian p spełnia warunek wyżej (jest prymitywny). Sprawdź przy pomocy komputera że dla $k = 7$, $l = 3$, $m = 2$ wielomian p spełnia powyzszy warunek. żywając komputera sprawdź że prostsze wielomiany stopnia 16 (tzn. mające mniej niż 5 niezerowych wyrazów) nie działają (nie są nieprzywiedlne). Uwaga: `irreducibe?(p::SUP(PF 2))` sprawdza czy wielomian jest nieprzywiedlny nad ciałem dwuelementowym. `primitive?` sprawdza czy wielomian jest prymitywny (można to też sprawdzić bezpośrednio rozkładając $2^{16} - 1$ na czynniki i obliczając odpowiednie potęgi w ciele skończonym).

16. Popularna suma kontrolna CRC działa następująco. Najpierw wybiera się wielomian prymitywny (patrz poprzednie zadanie) P nad ciałem dwuelementowym. Z ciągu bitów $b_0 b_1 \dots b_n$ produjemy wielomian $Q = \sum b_i x^i$. Następnie obliczamy resztę R z dzielenia Q przez P i traktujemy ją jako ciąg bitów. Uzasadnij że jeśli P jest wielomianem stopnia m spełniającym warunki poprzednigo zadania to CRC wykryje dowolną zmianę mniej niż m kolejnych bitów (tzn. otrzymamy różne R). Jeśli $n < 2^m$ to CRC wykryje dowolną zmianę dwu bitów.

Wskazówka: Co można powiedzieć o rozkładzie na czynniki wielomianu $x^k + x^l$?