1. Można pokazać że jeśli $P(x) = \sum_{i=0}^{m} a_i$, $Q(x) = \sum_{i=0}^{n} b_i$, a_i i b_i są całkowite, $k = \min(n, m)$, $A = \max\{|a_i|\}$, $B = \max\{|b_i|\}$, to współczynniki największego wspólnego dzielnika P i Q są ograniczone przez $C = 2^k \min((m+1)A, (n+1)B)$. Oznacza to że jeśli $a_m = 1$, $b_n = 1$, $p > 2C$ i największy wspólny dzielnik P i Q modulo p ma taki sam stopień jak największy wspólny dzielnik nad liczbami całkowitymi to współczynniki największego wspólnego dzielnika nad liczbami całkowitymi można odczytać z wyniku modulo p. Oszacuj koszt takiego obliczenia i porównaj z obliczeniem bazowanym tylko na arytmetyce całkowitoliczbowej.

2. Wylicz współczynniki $c_1, c, 2$ takie że jeśli $x = n_1 \mod 1234$ i $x = n_2 \mod 1111$ to $x = c_1 n_1 + c_2 n_2 \mod 1370974$

3. Niech $P_1 = x^4 + 11x^3 + 13x^2 + 150x + 77$, $P_2 = x^3 + 18x^2 + 73x - 44$. Oblicz wspólny dzielnik P_1 i P_2 po redukcji współczynników modulo $p = 3, 31, 37$. Znajdź wspólny dzielnik P_1 i P_2 nad liczbami całkowitymi bazując na wynikach obliczeń modularnych.

Uwaga: Potrzebne obliczenia wspólnych dzielników nad ciałami skończonymi najlepiej wykonać przy pomocy komputera. Np. w systemie FriCAS polecenia niżej dają wynik dla $p = 3$:

```
p1 := x^4 + 11*x^3 + 13*x^2 + 150*x + 77
p2 := x^3 + 18*x^2 + 73*x - 44
ppF := UP(x, PF 3)
gcd(p1::ppF, p2::ppF)
```

Powyżej `UP(x, PF 3)` oznacza wielomiany zmiennej o współczynnikach z ciała 3 elementowego (czyli Z_3), zaś `::` jest operatorem konwersji (koercji) do zadanego typu.

4. Niech $M = p_1 p_2 \ldots p_k$, gdzie p_i są parami względnie pierwszymi liczbami mieszczącymi się w słowie maszynowym komputera. Niech A i B będą macierzami całkowitoliczbowymi n na n o elementach co do warości bezwględnej mniejszych od m, przy tym $2nm^2 < M$. Uzasadnij że produkt maciery AB można obliczyć modulo p_i, $i = 1, \ldots, k$ a następnie zrekonstuować używając chińskie twierdzenie o resztach. Porównaj koszt takiego obliczenia z bezpośrednim obliczeniem produktu. Uwaga: zakładamy że produkt macierzy i produkty liczb obliczamy używając szkolne (naiwne) metody.

5. Niech

$$A = \begin{pmatrix} 4 & 17 \\ 3 & 11 \end{pmatrix}$$

Rozwiąż układ równań $Ax = y$ gdzie $y = (7, 0)$ obliczając rozwiązanie modulo 5 i modulo 11 i stosując chińskie twierdzenie o resztach. Uwaga: rozwiązanie modulo 5 można obliczyć w systemie FriCAS poleceniami niżej:

```
A := matrix([[4, 17], [3, 11]])
y := vector([7, 0])
solve(A::Matrix(PF(5)), y::Vector(PF(5)))
```

6. Niech p będzie liczbą pierwszą zaś K będzie ciałem skończonym mającym p^m elementów. Uzasadnij że jeśli $k(p^m - 1) + lp = 1$ to x^l jest pierwiastkiem stopnia p z x, tzn. $(x^l)^p = x$ dla dowolnego x z K. Jak można znaleźć l?

7. Znajdź pierwiastek stopnia 1024 z jedynki modulo 12289, tzn. liczbę a taką że $a^{1024} = 1 \mod 12289$. Zrób to na dwa sposoby, w pierwszym wykonaj obliczenia krok po kroku używając komputer co najwyżej do mnożenia i dzielenia modulo. Pokaż jak to zrobić jednym poleceniem dla komputera.

8. Zakładamy że $a^N = 1$ (dla pewnego ustalonego N). Mówimy że wektor $(c_j)_{j=0}^{N-1}$ jest dyskretną transformacją Fouriera wektora $(b_i)_{i=0}^{N-1}$ gdy

$$c_j = \sum_{i=0}^{N-1} b_i a^{ij}$$

piszemy też wtedy $DFT(b) = c$. Sprawdź że wtedy

$$Nb_i = \sum_{j=0}^{N-1} c_j a^{-ij}.$$

Uzasadnij że jeśli b_i traktujemy jako współczynniki wielomianu to $DFT(b)$ to obliczanie wartości w pierwiastkach z 1.

9. Stosujemy oznaczenia z poprzedniego zadania. Uzasadnij że jeśli $P(x) = \sum_{i=0}^{N} v_i x^i$, $Q(x) = \sum_{i=0}^{N} u_i x^i$ i $R = PQ \mod x^N - 1$ i $R(x) = \sum_{i=0}^{N} w_i x^i$, to

$$DFT(w) = DFT(v)DFT(u)$$

gdzie monożenie jest po składowych. Oznacza to że DFT można użyć by sporowadzić mnożenie wielomianów do mnożenia skalarów.

10. Stosujemy oznaczenia z poprzednich zadań. Uzasadnij że jeśli $N = ML$ to biorąc $i = Ml + k$, $j = Lm + n$ mamy

$$c_j = \sum_{k=0}^{M-1} (a^L)^{mk} a^{nk} \sum_{l=0}^{L-1} b_{Ml+k} (a^M)^{ln}.$$

Uzasadnij że powyższe wyrażenie można obliczyć jako M aplikacji DFT długości L, mnożenie po składowych wektorów długości N i L aplikacji DFT długości M. Rekursywnie stosując ten wzór DFT można obliczać przy pomocy $O(n \log(n))$ operacji. Działa to zarówno dla arytmetyki zespolonej jak i dla modularnej.

11. Uzasadnij że mnożenie liczb nm-bitowych można sprowadzić do mnożenia wielomianów stopnia $n-1$ o współczynnikach m-bitowych kosztem liniowej względem rozmiaru danych ilości operacji. Uzasadnij że procedurę mnożenia liczb nk-bitowych gdzie $k = \log_2(n) + 2m + 1$ można użyć do mnożenia wielomianów stopnia $n-1$ o współczynnikach m-bitowych kosztem liniowej względem rozmiaru danych ilości operacji.

Wskazówka: Zapisz liczby przy podstawie 2^m, popatrz jak wyglądają operacje i co się dzieje z przeniesieniami.

12. Uzasadnij że jeśli naszym pierścieniem są liczby całkowite modulo $K = 2^N - 1$, zaś $a = 2$ to DFT można obliczać używając tylko dodawanie, odejmowanie, przesunięcia bitowe i porównania (tzn. nie używając mnożenia ani dzielenia). Uzasadnij że takie DFT plus liniowa ilość dodatkowych operacji pozwala sprowadzić mnożenie liczb długości $N(N - \log_2(N) - 1)/4$ do N mnożeń liczb długości N.

Uwaga: Jest to kluczowy krok procedury Schoenage-Strassena.