Мои контакты: Алексей Давыдов <adavydow@gmail.com>
Задачи можно сдавать мне на почту или письменно до конца курса.
Задачи с практики сдавать, естественно, не надо.

Математика

Практика

Алгоритм Евклида

1. Вот обычный (но медленный) алгоритм Евклида:

   $\gcd(x, y) =$

   - $x < y : \gcd(x, y - x)$
   - $x > y : \gcd(x - y, y)$
   - $x = y : \frac{x+y}{2}$

   Расширим его так:

   $\gcd+(x, y, u, v) =$

   - $x < y : \gcd+(x, y - x, u, y + v)$
   - $x > y : \gcd+(x - y, y, u + v, v)$
   - $x = y : (\frac{x+y}{2}, \frac{u+v}{2})$

   Что за пара будет в ответе, при запуске $\gcd+(x, y, x, y)$? Оцените ассимптотику такого алгоритма.

2. А вот быстрый алгоритм Евклида:

   $\gcd(x, y) =$

   - $x < y : \gcd(x, y\%x)$
   - $x > y : \gcd(x\%y, y)$
   - $x = y : x$

   Оцените его асимптотику. Как нужно изменить этот алгоритм, если мы хотим не только найти $\gcd(u, v)$, но и такие числа x, y, что $ux + vy = gcd(x, y)$

3. Докажите, что следующий алгоритм находит gcd двух чисел:

   $\gcd(x, y) =$

   - $x = y : x$
   - $2 \mid x \wedge 2 \mid y : 2 \times \gcd(\frac{x}{2}, \frac{y}{2})$
   - $2 \mid x \wedge 2 \nmid y : \gcd(\frac{x}{2}, y)$
   - $2 \nmid x \wedge 2 \mid y : \gcd(x, \frac{y}{2})$
   - $x > y : \gcd(x - y, y)$
   - $x < y : \gcd(x, y - x)$

   Оцените его асимптотику. Как обобщить его на многочлены? Как нужно изменить этот алгоритм, если мы хотим не только найти $\gcd(u, v)$, но и такие числа (многочлены) x, y, что $ux + vy = gcd(x, y)$

Корни многочлена

4. Алгоритм поиска квадратного корня из a по модулю p такой: $\mathrm{root}(a, p) =$

   - $x\%4 = 3 : a^{\frac{p+1}{4}}$
   - иначе : выбираем ρ
     - считаем p:= $\gcd((x-\rho)^2 - a, x^{\frac{p-1}{2}} - 1)$
       - p = x - g : $g - \rho$ или $g + \rho$ ответ
       - иначе : поворяем с новым ρ

   Если вероятность угадать хорошее ρ не менее $\frac{1}{2}$ то какова сложность данного алгоритма?

5. Докажите, что $\prod\limits_{a \in \mathbb{Z}_p} (x - a) = x^p - x$

6. Корни квадратных и линейных многочленов мы находить умеем, а какнайти корни произвольного многочлена?

   Нам понадобится обощение недоказанного факта из задачи 4 (его так же не будем доказывать): Для больших простых p для произвольного множества $A \subset \mathbb{Z}_p^*$ и случайного a, рассмотрим множество $A + a = \{x + a \mid x \in a\}$. Вероятность того, что $|(A + a) \cap QR_p| \in [\frac{A}{4}, \frac{3A}{4}]$, не менее $\frac{3}{4}$ (QR_p — множество квадратичных вычетов в $\mathbb{Z}_p^*$).

Решето Эратосфена

7. Линейное решето Эратосфена.

Разложение на множители

8. ρ-метод Полларда.
9. Почему линейная функция в ρ-методе — плохо.
10. Пример немногочлена для метода Полларда.

Примитивный элемент в $\mathbb{Z}_p^*$

11. Пусть известна факторизация $p - 1$.

    - Придумайте алгоритм, который проверяет, являетря ли $g \in \mathbb{Z}_p^*$ генератором. Оцените сложность данного алгоритма.
    - Какова вероятность того, что случайно выбранный элемент из $\mathbb{Z}_p^*$ является генератором?
    - Придумайте алгоритм поиска генератора. Какова его сложность?

12. Пусть нам известо, что $p - 1 = wq$, где w — B-гладкое, а все простые делители q больше B. Придумайте алгоритм, который сможет найти генератор с вероятностью не менее $\frac{\log_2 p}{B \log_2 B}$. Какова его сложность? А если разложение заранее не известно, сколько времени займет поиск генератора с заранее заданной точностью?

Задачи для самостоятельного решения

1. Пусть мы умеем умножать два многочлена степени n за время $M(n)$. Вам даны два многочлена x и y степени n. Придумайте, как найти такие a и b, что $ax+by = gcd(x, y)$ за $O(nM(n))$ (Подсказка: придумайте, как расширить алгоритм из задачи 3).

2. Одним из фактов, используемых ρ методом Полларда для разложения на множители является то, что функция $f(x) = x^2 + a : \mathbb{Z}_n \to \mathbb{Z}_n$ обладает следующим свойством: для каждого делителя d числа n мы имеем, что из $u \equiv v \mod d$ следует, что $f(u) \equiv f(v) \mod d$. Докажите, что это свойство выполняется для любого многочлена. Приведите пример немногочленеа, для которого выполнено это свойство.

3. Пусть G — циклическая группа порядка n с образующим g и элементом t. Пусть мы нашли такие числа a и b, что $g^b = t^a$. Предложите алгоритм поиска дискретного логарифма l, за время $O(gcd(a, n) \times poly(n))$.