Тексты на диске O: Irreducibility Tests in $\mathbf{F}_p[T]$

1. Докажите малую теорему Ферма в $\mathbf{F}_p[T]$: если $\pi \in \mathbf{F}_p[T]$ неприводим и $a \in \mathbf{F}_p[T]$ удовлетворяет условию НОД$(a, f) = 1$, то $a^{\mathrm{N}(f)-1} \equiv 1 \bmod f$.

2. Определите, какие из этих 9 многочленов в $\mathbf{F}_3[T]$ неприводимы: $T^2 + 1$, $T^2 + 2$, $T^2 + 2T + 1$, $T^2 + 2T + 2$, $T^3 + T + 2$, $T^3 + 2T + 2$, $T^4 + 1$, $T^4 + 2T + 1$, $T^4 + 2T + 2$. (Ответы: 4 прив., 5 неприв.)

3. Для нечетного простого p и $f \in \mathbf{F}_p[T]$ проверьте, что $\mathrm{N}(f) \equiv 1 \bmod 4 \iff$ (i) $p \equiv 1 \bmod 4$ или (ii) $p \equiv 3 \bmod 4$ и $\deg f$ четное.

4. Вычислите символы Лежандра $\left(\dfrac{T^2+1}{T^3-T+1}\right)$ в $\mathbf{F}_3[T]$ и $\left(\dfrac{2T^2+1}{T^3+T+1}\right)$ в $\mathbf{F}_5[T]$. (Ответы: -1, 1)

5. а) Для целого $k \geq 2$ и целых $m, n > 0$ докажите, что $(k^m - 1) \mid (k^n - 1) \iff m \mid n$.

   б) Докажите критерий Корсельта в $\mathbf{F}_p[T]$: приводимый многочлен $f \in \mathbf{F}_p[T]$ является многочленом Кармайкла тогда и только тогда, когда (i) f свободен от квадратов (т.е., f не делится на квадрат никакого непостоянного многочлена) и (ii) если неприводимый многочлен π делит f, то $\deg \pi \mid \deg f$ (что эквивалентно, по пункту а, $(\mathrm{N}(\pi) - 1) \mid (\mathrm{N}(f) - 1)$).

   в) Проверьте, что произведение $f = \pi_1\pi_2$ двух различных неприводимых многочленов является многочленом Кармайкла тогда и только тогда, когда $\deg \pi_1 = \deg \pi_2$.

6. Докажите теорему Соловея–Штрассена для неприводимых многочленов $f \in \mathbf{F}_p[T]$, где $p \neq 2$: существует такой $a \in \mathbf{F}_p[T]$, что $\deg a < \deg f$, НОД$(a, f) = 1$, и $a^{(\mathrm{N}(f)-1)/2} \not\equiv (\frac{a}{f}) \bmod f$. Выведите отсюда, что плотность свидетелей Эйлера f больше 50%.

7. Докажите, что константы $c \in \mathbf{F}_p^\times$ ($p \neq 2$) не являются свидетелями Эйлера. Это аналог того, что ± 1 в $\mathbf{Z}$ не являются свидетелями Эйлера.

8. Докажите, что каждый неприводимый многочлен в $\mathbf{F}_p[T]$ ($p \neq 2$) не имеет никаких свидетелей Миллера–Рабина.

9. Прочитайте (в тексте о тесте Миллера–Рабина) доказательство теоремы о том, что плотность свидетелей Миллера–Рабина всякого нечетного составного n всегда больше 75%, кроме случая равенства при $n = 9$.

   а) Переведите рассуждение в контекст $\mathbf{F}_p[T]$ ($p \neq 2$), чтобы доказать аналог для приводимых многочленов, которые *не* многочлены Кармайкла вида $\pi_1\pi_2$. В частности, плотность равна 75% только когда $p = 3$ и $f = (T + c)^2$, где $c \in \mathbf{F}_3$.

   б) Что можно сказать о плотности свидетелей Миллера–Рабина, когда $f = \pi_1\pi_2$ и $\deg \pi_1 = \deg \pi_2$? (Это многочлен Кармайкла в $\mathbf{F}_p[T]$ *без* аналога в $\mathbf{Z}$.)