Name: .... 27 Jan 2015

Studienkennzahl: ....

Matrikelnummer: ....

Final Exam
Computer Algebra (326.010)
(no books allowed)

(1) What is wrong with this attempt at a modular algorithm for computing the greatest common divisor of polynomials over $\mathbb{Z}$?

---

algorithm GCD_MOD(**in:** a, b; **out:** g);
$[a, b \in \mathbb{Z}[x]^*$ primitive, $g = \gcd(a, b)$.
Integers modulo m are represented as $\{k \mid -m/2 < k \leq m/2\}$.]
(1) $M := 2 \cdot (\text{Landau} - \text{Mignotte} - \text{bound for } a, b)$;
[in fact any other bound for the size of the coefficients can be used]
(2) $p :=$ a new prime;
$g_{(p)} := \gcd(a_{(p)}, b_{(p)})$;
(3) **if** $\deg(g_{(p)}) = 0$ **then** $\{g := 1$; **return**$\}$;
$P := p$;
$g := g_{(p)}$;
(4) **while** $P \leq M$ **do**
$\{p :=$ a new prime;
$g_{(p)} := \gcd(a_{(p)}, b_{(b)})$;
if $\deg(g_{(p)}) < \deg(g)$ **then goto** (3);
if $\deg(g_{(p)}) = \deg(g)$
then $\{g := \text{CRA\_2}(g, g_{(p)}, P, p)$;
[actually CRA_2 is applied to the coefficients of g and $g_{(p)}$]
$P := P \cdot p \ \} \}$;
(5) $g :=$ primitive part of g;

---

(2) Consider $a(x) = 6x^4 + 13x^3 + 14x^2 + 8x + 1$.
(a) Is a squarefree in $\mathbb{Q}[x]$?
(b) Is a squarefree in $\mathbb{Z}_5[x]$?
(c) Are there finitely many or infinitely many primes p such that a is not squarefree in $\mathbb{Z}_p[x]$?
(d) How can one determine those primes p for which a is not squarefree in $\mathbb{Z}_p[x]$?

(3) Factorization in $\mathbb{Z}_p[x]$, p a prime:
What are the main steps of the Berlekamp factorization algorithm?
Explain these main steps of the Berlekamp factorization algorithm.

(4) Prove or disprove the following statements:
(a) *Let $f(x), g(x) \in K[x]$, K a field. Then $\{\gcd(f,g)\}$ is a Gröbner basis for $\langle f, g\rangle$.*
(b) *Let $f(x,y), g(x,y) \in K[x,y]$, K a field. Then $\{\gcd(f,g)\}$ is a Gröbner basis for $\langle f, g\rangle$.*

(5) (a) Is $G = \{g_1, g_2\}$ a Gröbner basis for an ideal in $\mathbb{Q}[x,y]$ with respect to the lexicographic term ordering with $x < y$?

$$g_1 = y^2 + x^3 - 1, \qquad g_2 = x^4 + x^2 + 1$$

(b) How many complex solutions (counting multiplicities) does the system of equations $g_1(x,y) = g_2(x,y) = 0$ have?
(c) How would a Gröbner basis for an ideal in $\mathbb{Q}[x,y]$ have to look like, so that the corresponding system of equations has infinitely many complex solutions?