Číslo cvičení: 8
Jméno: Marek Bryša
UČO: 323771
Login: xbrysa1

1. $$n^{40}+1=(n^8)^5+1=x^5+1=(x+1)\cdot(x^4-x^3+x^2-x+1)$$

2. $4a^3+27b^2 \mod p \neq 0 \iff$ elliptic curve can be used to form a group over F_p.
   $4\cdot 1000+27\cdot 25 \mod 17=0 \implies$ the e.c. does not form the group.

3. (a) $a_1=3^2+1 \mod 4577=10$, $b_1=(3^2+1 \mod 4577)^2+1 \mod 4577=101$, $gcd(10-101,4577)=1$
   $a_2=10^2+1 \mod 4577=101$, $b_1=(101^2+1 \mod 4577)^2+1 \mod 4577=4402$, $gcd(101-4402,4577)=23$
   $4577=23\cdot 199$

   (b) $2P=(80,65)$ and we compute $gcd(283,143)=1$.
   $3P=(131,102)$ and we compute $gcd(64,143)=1$.
   $4P=(14,28)$ and we compute $gcd(13,143)=13$.

4. The elliptic curve is isomorphic to Z_5. ∞ has the role of 0.

+	∞	(0,1)	(0,6)	(4,2)	(4,5)
∞	∞	(0,1)	(0,6)	(4,2)	(4,5)
(0,1)	(0,1)	(4,5)	∞	(0,6)	(4,2)
(0,6)	(0,6)	∞	(4,2)	(4,5)	(0,1)
(4,2)	(4,2)	(0,6)	(4,5)	(0,1)	∞
(4,5)	(4,5)	(4,2)	(0,1)	∞	(0,6)

5. $x^{11}-1=0 \mod 2011 \iff x^{11}=1 \mod 2011$. From Euler's theorem $a^{\varphi(n)}=1 \mod n$ if a is coprime to n and here all are, since n is prime. $\varphi(2011)=2010=2\cdot 3\cdot 5\cdot 67$. In case of a prime exponent, the solution to the original equations other than $x=1$ only exist for prime factors of 2010. 11 is not one of them so the solution does not exist.