

# Comments on some Oral Practice Problems

November 19, 2011

Here are some additional comments on my list of oral problems.

1. First a word on the Chinese Remainder theorem, let's take the relation  $p \equiv 7 \pmod{8}$  and  $p \equiv 1 \pmod{5}$ . If you want to find the (unique) congruence class  $\pmod{40}$ , there is a procedure to do that rather than listing everything, the situation is a bit more general:

Take pairwise coprime numbers  $m_1, m_2, \dots, m_n$ , define  $M_i := \prod m_1 \cdots \hat{m}_i \cdots m_n$ , and  $M_i^{-1}$  is any number that represents the inverse of  $M_i \pmod{m_i}$ . Then the solution of the system of congruence relations  $p \equiv a_1 \pmod{m_1}, \dots, a_n \pmod{m_n}$  is equal to  $\sum a_i M_i M_i^{-1} \pmod{\prod m_i}$ .

2. For the question of asking "for which primes  $p$  is 10 a fourth power modulo  $p$ ?", of course, if you want to give an answer in terms of congruence relations, the ultimate congruence relation should come from class field theory. First let's just see how much one can see with naked eyes. If  $p = 4k + 3$ , then if 10 is a square it is automatically a fourth power. (Why?) But if 10 is not a square, -10 is. So 10 is a fourth power anyway. If  $p = 4k + 1$ , the situation is a bit more complicated.

The Galois group of the splitting field  $K = \mathbb{Q}(i, \sqrt[4]{10})$  of  $x^4 - 10 = 0$  over  $\mathbb{Q}$  is the dihedral group of order 8. It is order 8 group, and not abelian, otherwise every subfield is Galois, which we know is not true. So the only candidate we have is the dihedral group  $D_4$  or the quaternion group. It is a cyclic quartic extension of  $\mathbb{Q}(i)$ , but not cyclic over the other two quadratic subfield, thus it is not the quaternion group. The four roots of  $x^4 - 10$  are  $\sqrt[4]{10}, i\sqrt[4]{10}, -\sqrt[4]{10}, -i\sqrt[4]{10}$ , call them  $\{1, 2, 3, 4\}$ . Given  $D_4$  the presentation  $\{\tau, \sigma \mid \tau^4, \sigma^2, \tau\sigma\tau\sigma\}$ , we can identify the action of  $D_4$  on  $(1, 2, 3, 4)$ . The four elements in  $D_4$  that each of them do not generate a normal subgroup of order 2 are the elements  $\sigma, \sigma\tau, \sigma\tau^2, \sigma\tau^3$ . Pick  $\tau$  for example, say it fixes  $\{1, 3\}$ , then it acts like  $(2, 4)$ .  $\tau$  acts like  $(1, 2, 3, 4)$ . (Of course this assignment is not canonical, everything is up to conjugation. I just use it to simplify the discussion.) Now you can see directly, the quadratic subfield  $\mathbb{Q}(i)$  is fixed by  $\{1, \tau, \tau^2, \tau^3\}$ ;  $\mathbb{Q}(\sqrt{10})$  is fixed by  $\{1, \sigma, \tau^2, \sigma\tau^2\}$ ;  $\mathbb{Q}(i\sqrt{10})$  is fixed by  $\{1, \tau^2, \sigma\tau, \sigma\tau^3\}$ . These three subfields are governed by the biquadratic field  $\mathbb{Q}(i, \sqrt{10})$  which is fixed by the commutator subgroup  $\{1, \tau^2\}$ . If you just adjoin one (then automatically its minus) roots of  $x^4 - 10$  to  $\mathbb{Q}$ , you can say that field is fixed by any one of the babies  $\sigma, \sigma\tau, \sigma\tau^2, \sigma\tau^3$ . i.e. you are looking for primes in  $\mathbb{Z}$  whose decomposition group is either trivial or contained in the order two subgroup generated by one of the above babies.

How much more information do you get than the naked eyes ?

Remark\*: If you care about the ramification index of 2 in  $\mathbb{Q}(i, \sqrt{10})$ , you can

ask whether it ramifies in  $\mathbb{Q}_2(i, \sqrt{10})/\mathbb{Q}_2(i)$ . Say I pick a uniformizer  $i - 1 =: \pi$  in  $\mathbb{Q}_2(i)$ . Then  $i = \pi + 1$ ,  $2 = \pi^2(1 + \pi)$ ,  $10 \equiv 1 + \pi + \pi^2 \pmod{\pi^5}$ , and  $10 \equiv 1 + \pi \pmod{\pi^5 + U_1^2}$ . The Hilbert symbol of 10 pairs with representatives of units in  $\mathbb{Q}_2(i)$  don't all give you 1, thus  $\mathbb{Q}_2(i, \sqrt{10})/\mathbb{Q}_2(i)$  ramifies.

You can also verify the situation by class field theory: the Norm subgroup of  $\mathbb{Q}_2(i, \sqrt{10})^*$  in  $\mathbb{Q}_2^*$  is contained in the norm subgroup of  $\mathbb{Q}_2(i)^*$  and  $\mathbb{Q}_2(\sqrt{10})^*$ , and those are two different subgroups of index 2, so their intersection is at most index 4. Therefore the ramification index of their compositum is 4. This argument applies in more general situations.

The total ramification index of 2 in  $K$  is 8, for 5 it is 4. In particular, if you want to know the minimal modulus of  $K$  above  $\mathbb{Q}(i, \sqrt{10})$ , it is a product of primes above 2 and 5. So if you are going after the situation for primes of the form  $4k + 1$ , you probably can not express it just in terms of modulus condition with rational integers. (If you do, please email me!)

3. On constructing  $S_3$  extensions over  $\mathbb{Q}_p$  where  $p \nmid 2$ . This uses the transfer map on class field theory. The transfer map deals with the situation when you have a tower of Galois extension:  $K \subset F \subset L$ , where  $H := \text{Gal}(L/F) < \text{Gal}(L/K) =: G$ . The situation is you want to go from  $G^{ab}$  to  $H^{ab}$ , please check the article on wikipedia on the group theoretic recipe. In particular, if  $H = [G, G]$ , the transfer map is trivial, a result due to Furtwangler. If  $G$  is abelian, then  $\text{Ver}(g) = (\bar{g})^{|G/H|}$  where  $\bar{g}$  is the image of  $g$  in  $H$ . (Why?) On the ideal class group side, the map goes from using an ideal of  $\mathcal{O}_K$  to generate an ideal in  $\mathcal{O}_F$ , which is perfectly legitimate. In the local field situation, you just take an element of  $K^*$  and view it as an element in  $F^*$ .

Books by Gras/Artin and Tate on class field theory has statements about the transfer (Verlagerung) map.